TrueCrypt اور اس کا استعمال

بسم اللہ الرحمٰن الرحیم

TrueCrypt اور اس کا استعمال

TrueCrypt وہ اوپن سورس سوفٹ ویئر ہے جس کی مدد سے کمپیوٹر میں ایسے کنٹیز (container) بنائے جا سکتے ہیں جن میں ڈیٹا اینکرپٹڈ حالت میں رکھا جا سکتا ہے۔ پھر ان کنٹینرز کو کہیں بھی کاپی کیا یا لیجایا جا سکتا ہے۔ یہ کنٹینرز ایک عام فائل کی طرح ہی ہوتے ہیں اور انہیں رکھنے کیلئے کسی سوفٹ ویئر کی ضرورت نہیں، البتہ انہیں کھولنے (یعنی decrypt کرنے) کیلئے TrueCrypt کی ضرورت پڑتی ہے۔ TrueCrypt پہلے سے پڑے ڈیٹا کو اینکریپٹ نہیں کرتا بلکہ جو کچھ اس کے کنٹینر میں ڈالا جاتا ہے یہ اُسے اینکریپٹ کر دیتا ہے۔ اس لیے جب ڈیٹا کنٹینر میں منتقل کر لیا جائے تو باہر پڑے اُس ڈیٹا کو محفوظ طریقے (جیسے اسرار المجاہدین کے استعمال) سے ڈیلیٹ کر دیا جانا چاہیئے۔

TrueCrypt سوفٹ ویئر on-the-fly اینکرپشن کرتا ہے۔ یعنی ڈیٹا عین اُس وقت انکریپٹ ہوتا ہے جب یہ کنٹینر میں ڈالا جا رہا ہوتا ہے، اور صرف اُسی وقت ڈیکرپٹ ہوتا ہے جب اُسے کنٹینر سے نکالا جاتا ہے، اور کمپیوٹر کی RAM میں ہی رہتا ہے جب تک کہ خود اُسے کہیں محفوظ نہ کیا جائے۔ یہاں تک کہ اگر کوئی کنٹینر میں پڑی ویڈیو چلاتا ہے تو TrueCrypt کی مدد سے جس قدر ویڈیو پلیئر کو دکھانے کیلئے ویڈیو درکار ہوتی ہے اتنی ساتھ ساتھ ویڈیو ڈیکرپٹ ہوتی رہتی ہے اور باقی کی تمام فائلیں کنٹینر میں اینکرپٹڈ حالت میں پڑی رہتی ہیں۔ ڈیٹا کسی بھی وقت کمپیوٹر میں ، ماسوائے RAM کے ، اور کہیں بھی ڈیکرپٹڈ حالت میں موجود نہیں ہوتا۔

TrueCrypt ڈاؤن لوڈ کیلئے اُن کی ویب سائٹ پر موجود ہے :

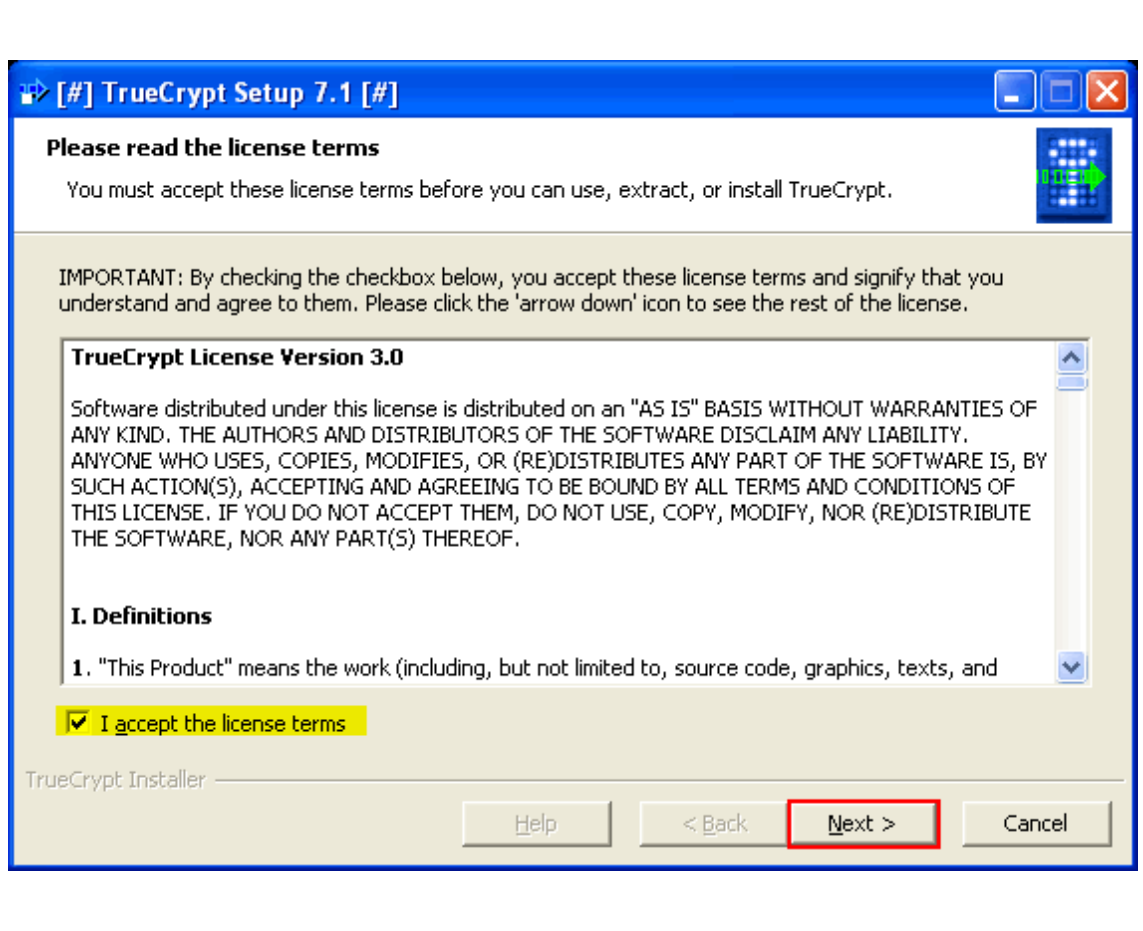
truecrypt.org/downloads

- TrueCrypt کی انسٹالیشن / ایکسٹریکشن
- کنٹینر بنانے کا طریقہ
- کنٹینر کھولنے (یعنی mount کرنے) کا طریقہ
- کنٹینر بند (یعنی dismount کرنے) کا طریقہ

TrueCrypt کی انسٹالیشن / ایکسٹریکشن

TrueCrypt انسٹال کیلئے اور پورٹیبل دونوں صورتوں میں دستیاب ہے۔ انسٹال کرنے کا طریقہ انتہائی آسان ہے۔ ذیل میں پورٹیبل ورژن کو extract کرنے کا طریقہ بتایا گیا ہے کیونکہ پورٹیبل کو استعمال کے بعد محفوظ طریقے سے بآسانی ڈیلیٹ کیا جاسکتا ہے اور اس طرح کمپیوٹر میں کوئی مواد / فائل / فنگر پرنٹ چھوٹ جانے کا ڈر نہیں رہتا جس سے یہ ذرا بھی معلوم ہو سکے کہ اِس کمپیوٹر میں کبھی TrueCrypt انسٹال یا استعمال ہوا تھا۔

TrueCrypt Setup 7.1.exe
TrueCrypt Setup
TrueCrypt Foundation


[#] TrueCrypt Setup 7.1 [#]

Please read the license terms

You must accept these license terms before you can use, extract, or install TrueCrypt.

IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

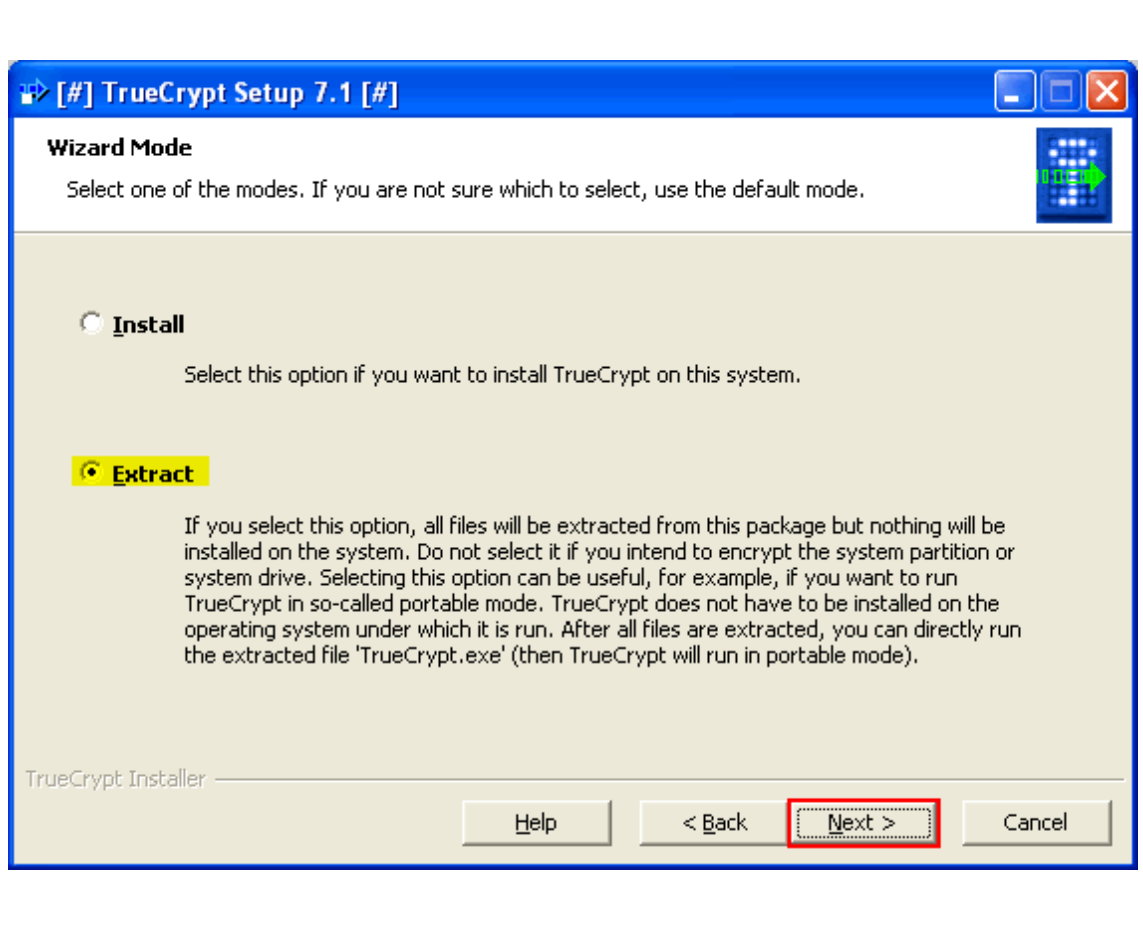
TrueCrypt License Version 3.0

Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, OR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.

I. Definitions

1. "This Product" means the work (including, but not limited to, source code, graphics, texts, and

☑ I accept the license terms


[#] TrueCrypt Setup 7.1 [#]

Wizard Mode

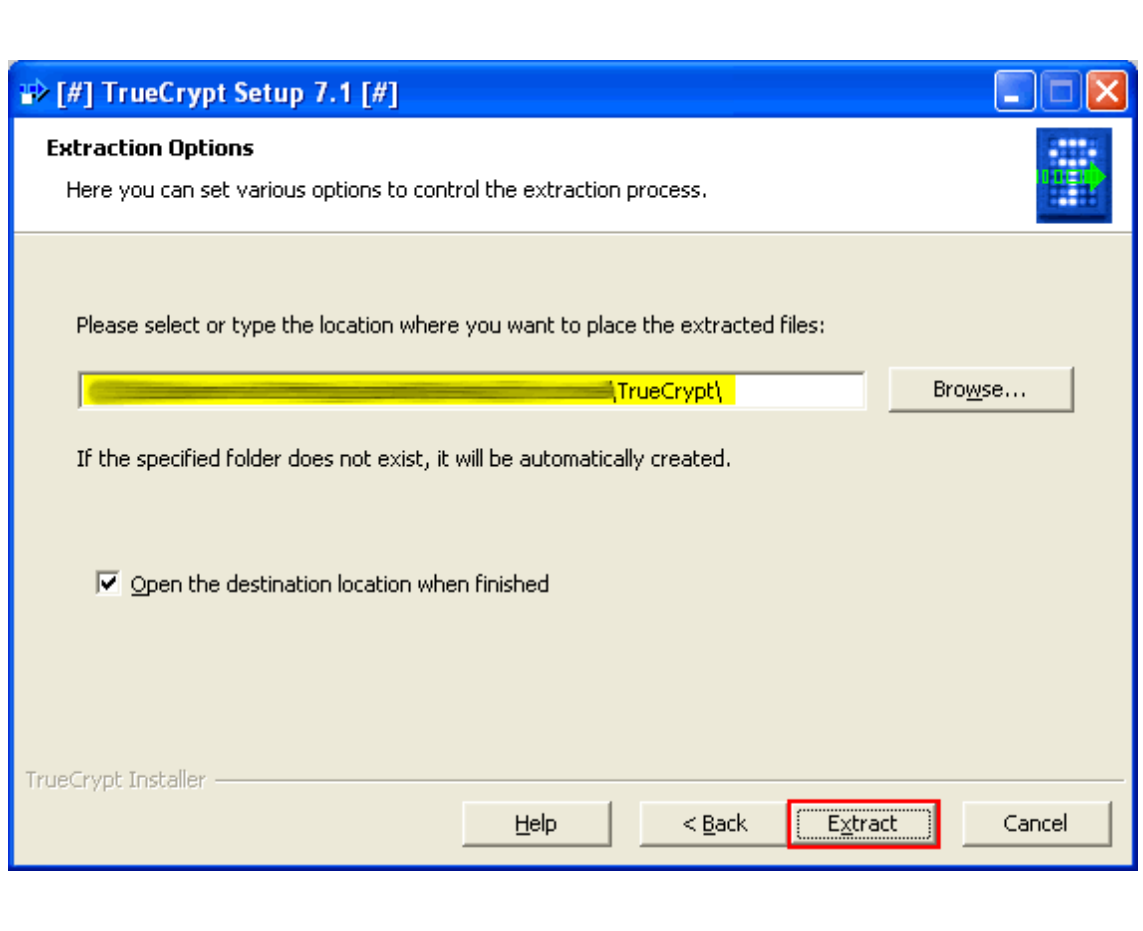
Select one of the modes. If you are not sure which to select, use the default mode.

○ Install

Select this option if you want to install TrueCrypt on this system.

● Extract

If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).


[#] TrueCrypt Setup 7.1 [#]

Extraction Options

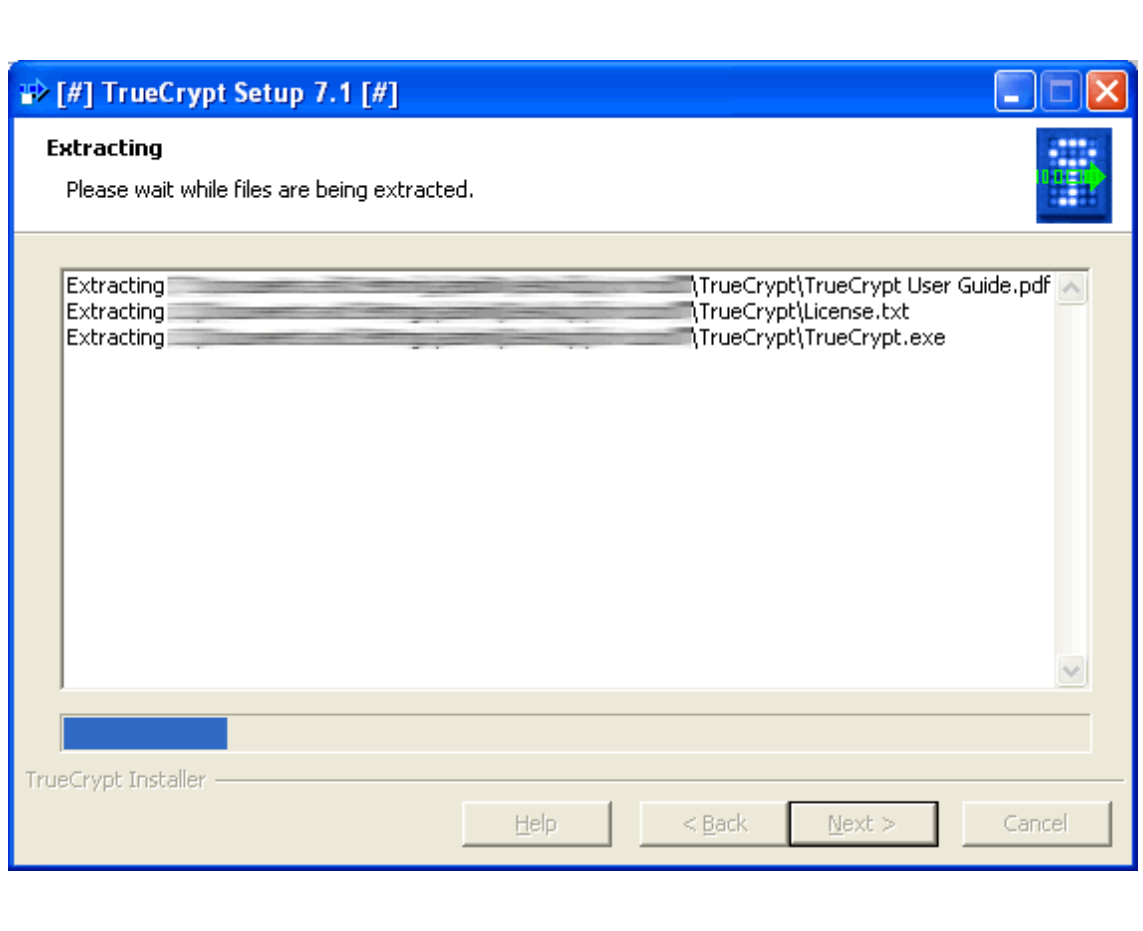
Here you can set various options to control the extraction process.

Please select or type the location where you want to place the extracted files:

[redacted]\TrueCrypt\

If the specified folder does not exist, it will be automatically created.

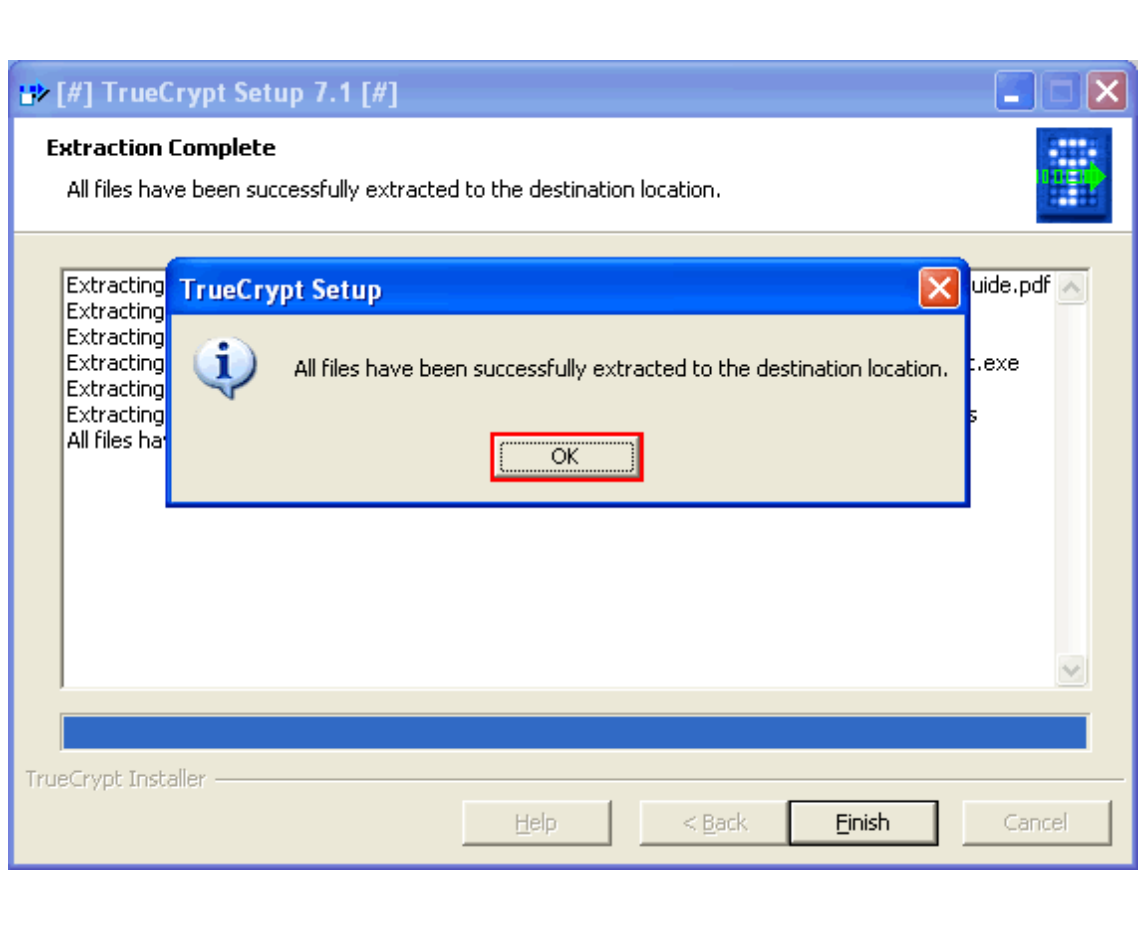
☑ Open the destination location when finished


[#] TrueCrypt Setup 7.1 [#]

Extracting

Please wait while files are being extracted.

Extracting [redacted]\TrueCrypt\TrueCrypt User Guide.pdf
Extracting [redacted]\TrueCrypt\License.txt
Extracting [redacted]\TrueCrypt\TrueCrypt.exe

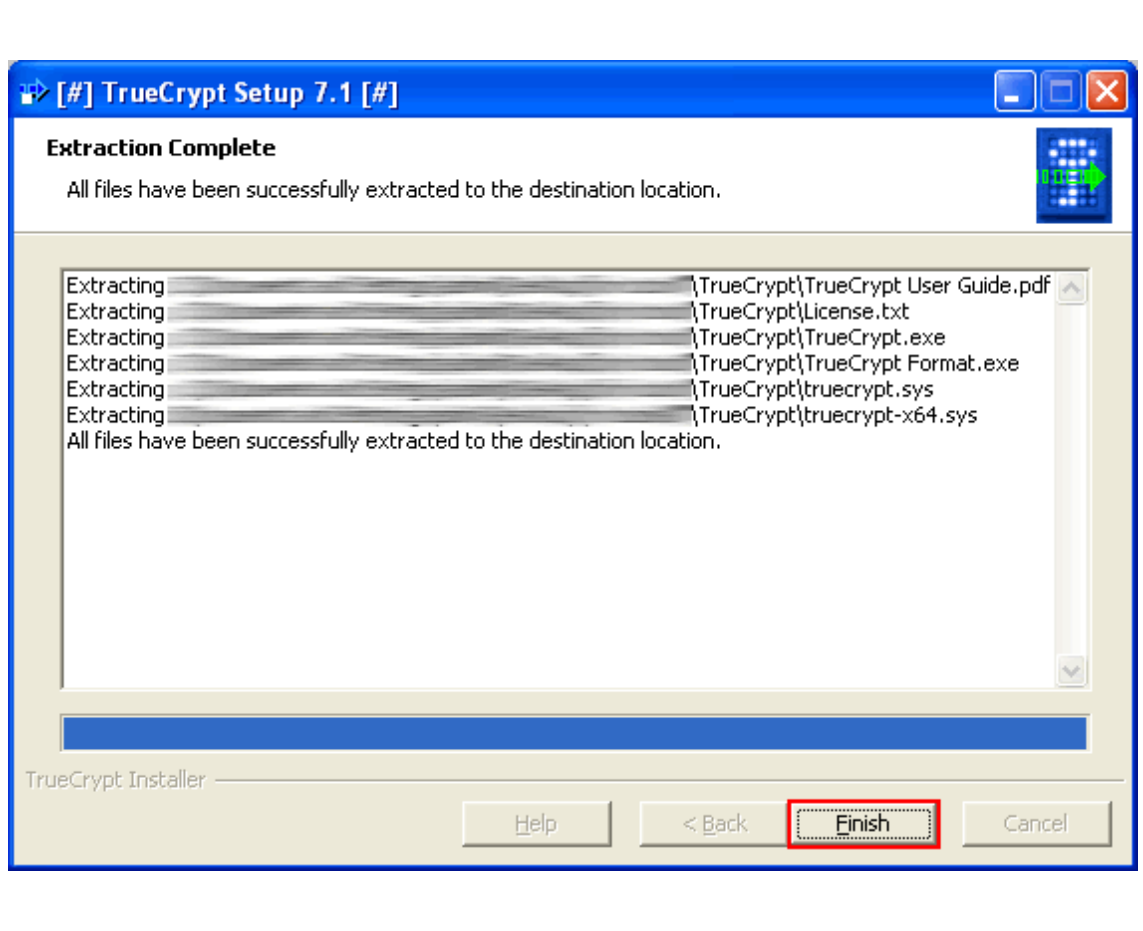

[#] TrueCrypt Setup 7.1 [#]

Extraction Complete

All files have been successfully extracted to the destination location.

TrueCrypt Setup

All files have been successfully extracted to the destination location.


[#] TrueCrypt Setup 7.1 [#]

Extraction Complete

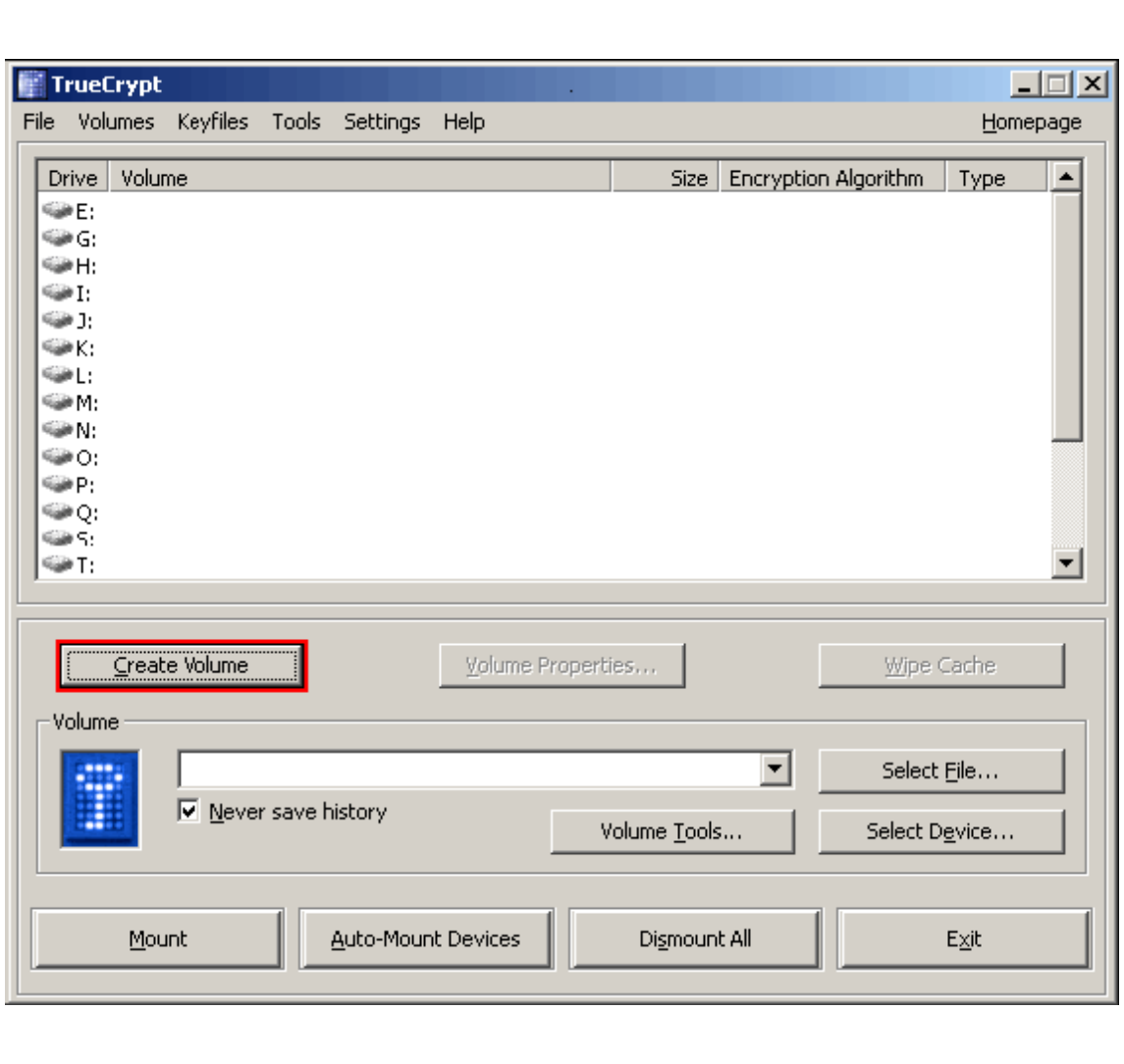
All files have been successfully extracted to the destination location.

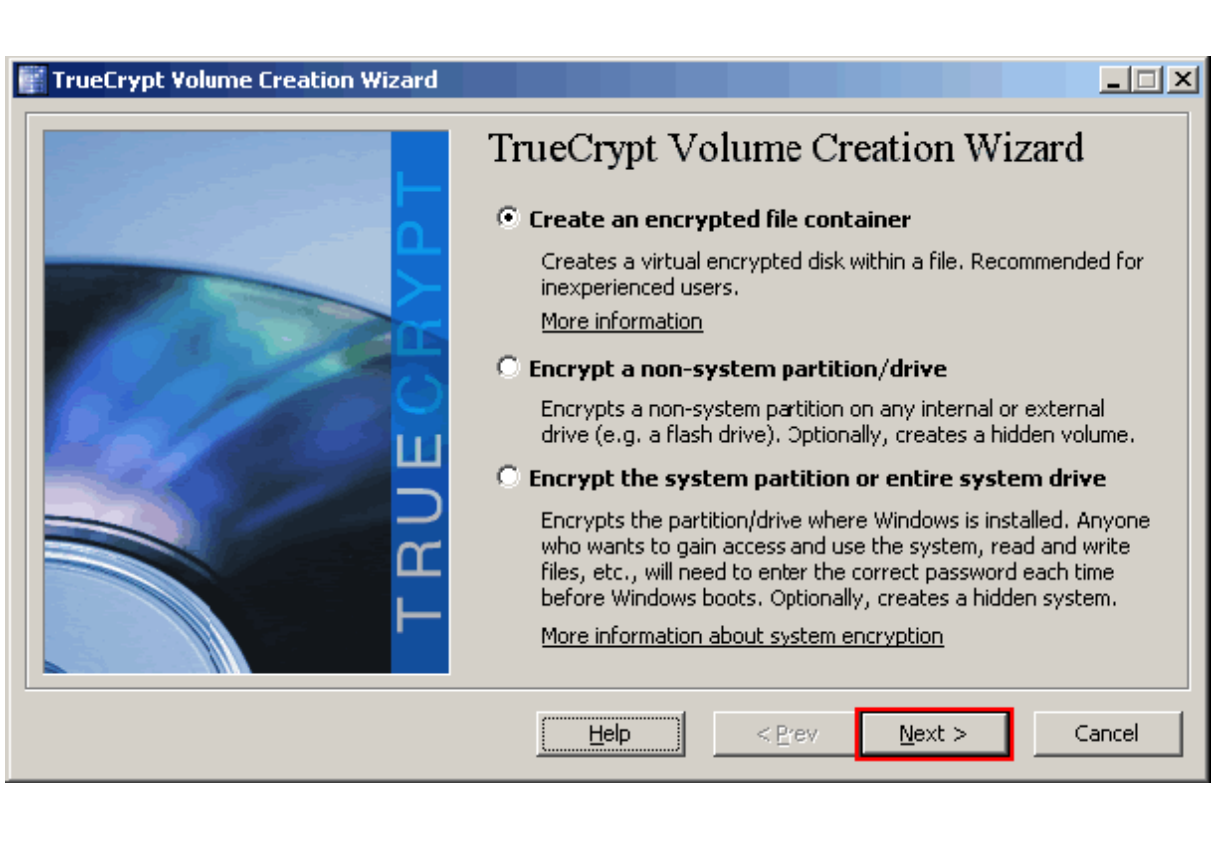
Extracting [redacted]\TrueCrypt\TrueCrypt User Guide.pdf
Extracting [redacted]\TrueCrypt\License.txt
Extracting [redacted]\TrueCrypt\TrueCrypt.exe
Extracting [redacted]\TrueCrypt\TrueCrypt Format.exe
Extracting [redacted]\TrueCrypt\truecrypt.sys
Extracting [redacted]\TrueCrypt\truecrypt-x64.sys
All files have been successfully extracted to the destination location.

TrueCrypt استعمال کیلئے ہماری بتائی گئی لوکیشن پر ایکسٹریکٹ ہو چکا ہے۔ استعمال کیلئے TrueCrypt.exe چلا لیں۔

TrueCrypt.exe

کنٹینر بنانے کا طریقہ


TrueCrypt


TrueCrypt Volume Creation Wizard

TrueCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

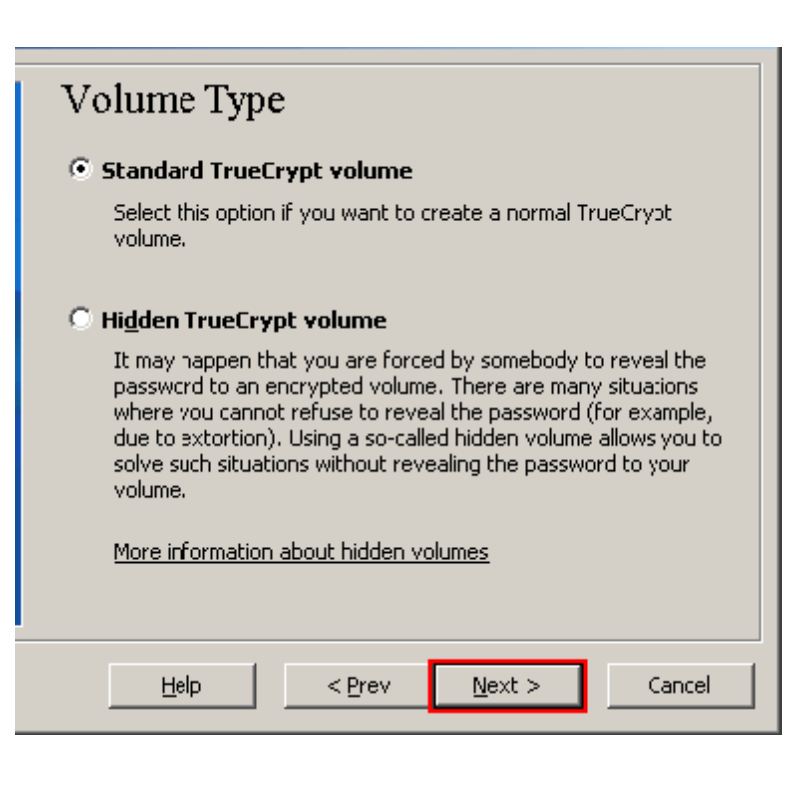
○ Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption


Volume Type

● Standard TrueCrypt volume

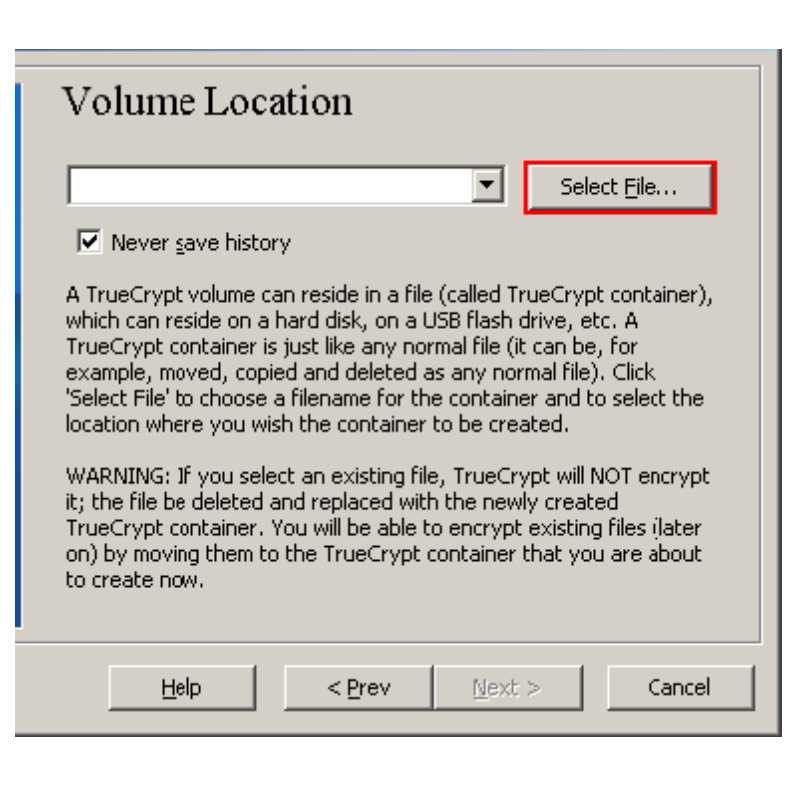
Select this option if you want to create a normal TrueCrypt volume.

○ Hidden TrueCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

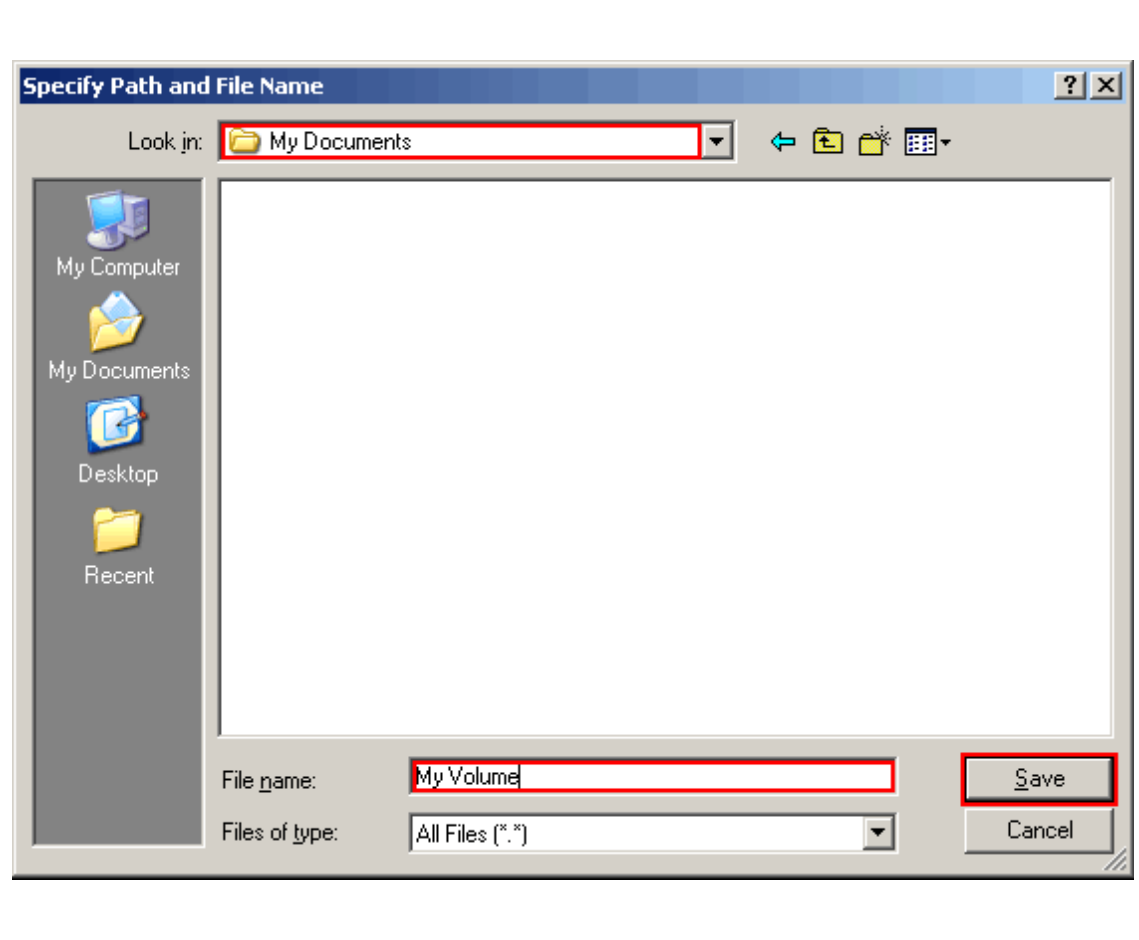
اب وہ لوکیشن بتائیں جہاں آپ کنٹینر بنانا چاہتے ہیں :


Volume Location

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

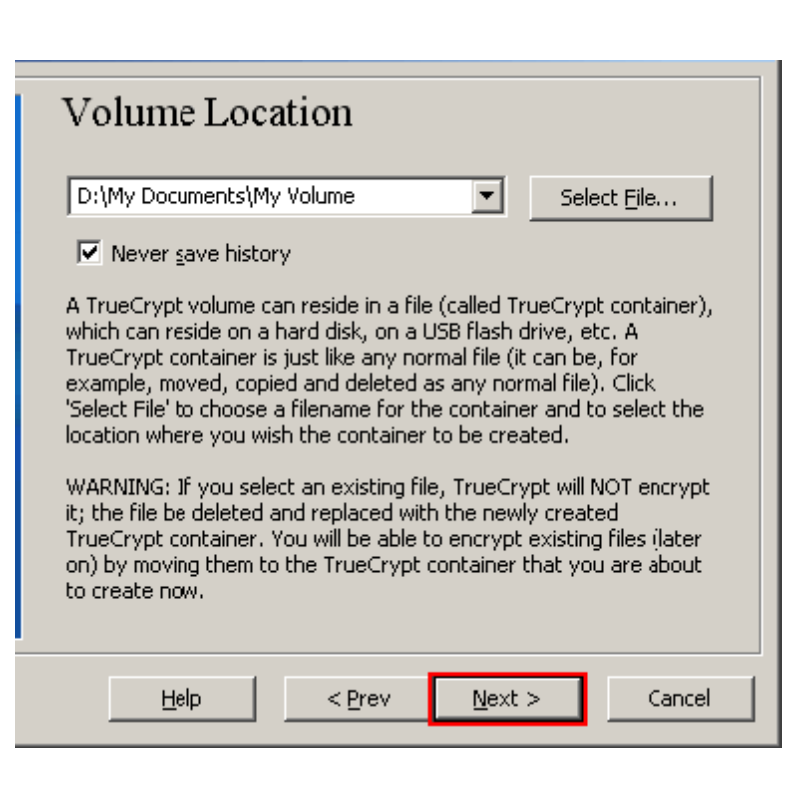
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.


Specify Path and File Name

Look in: My Documents

File name: My Volume

Files of type: All Files (*.*)

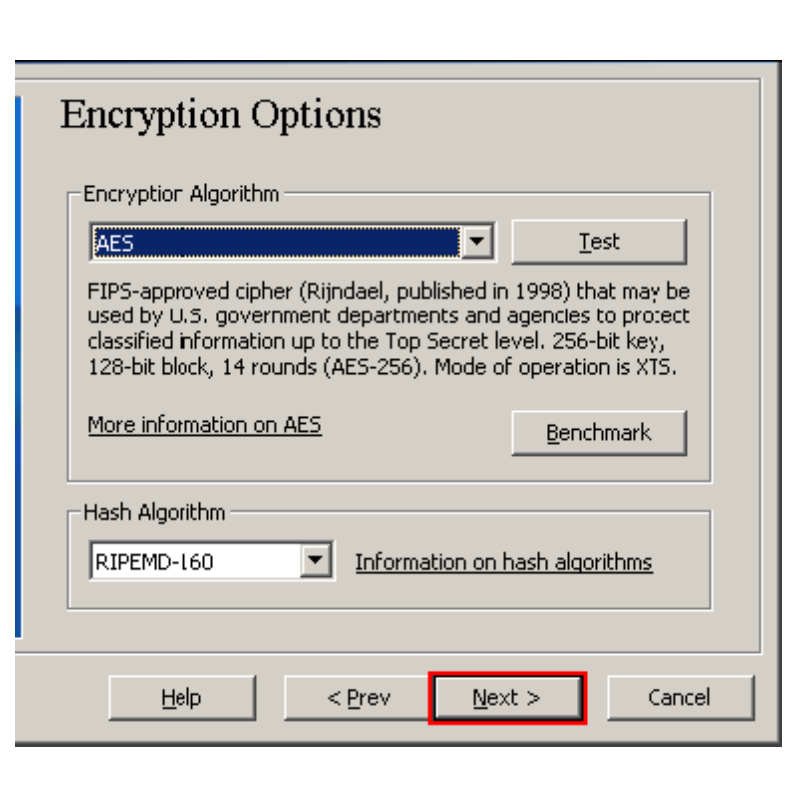

Volume Location

D:\My Documents\My Volume

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

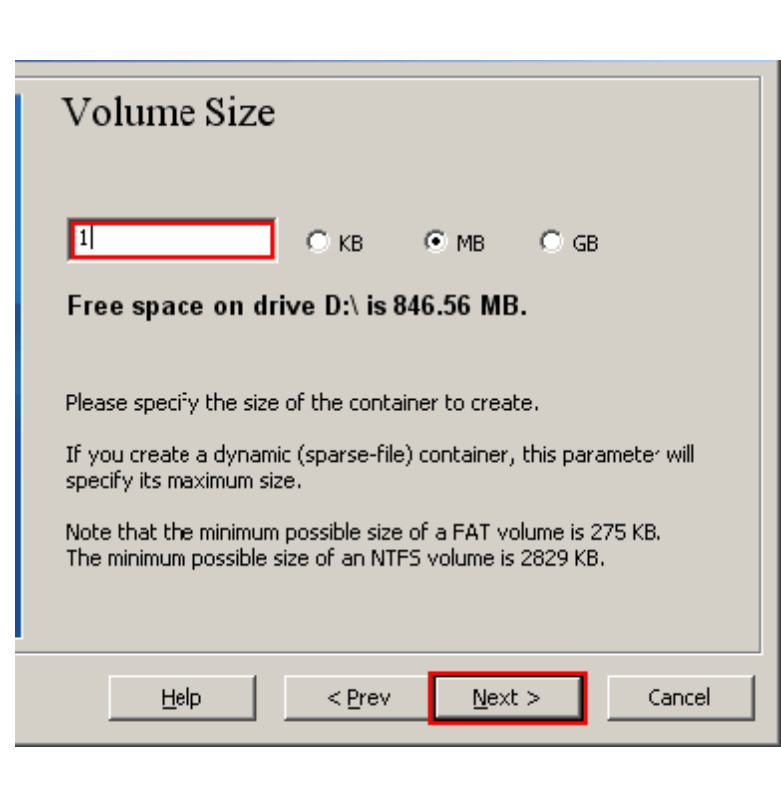

Encryption Options

Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: RIPEMD-160

جتنے سائز کا کنٹینر بنانا چاہتا ہیں، وہ بتائیں :


Volume Size

1 ○ KB ● MB ○ GB

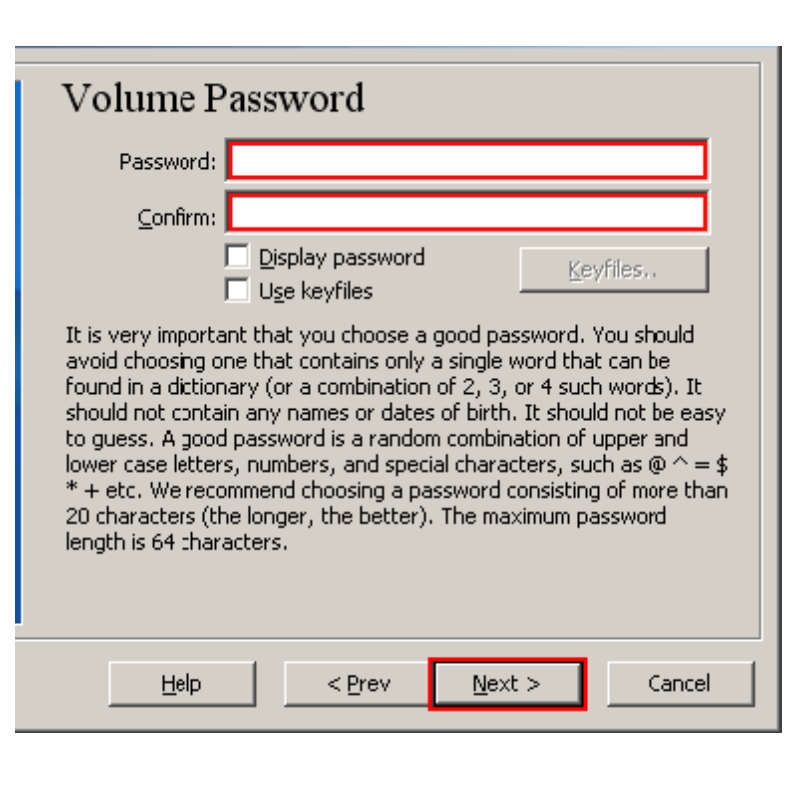
Free space on drive D:\ is 846.56 MB.

Please specify the size of the container to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum size.

Note that the minimum possible size of a FAT volume is 275 KB.
The minimum possible size of an NTFS volume is 2829 KB.

مضبوط پاسورڈ ڈالیں، پاسورڈ کم از کم ۲۰ حروف سے زیادہ پر مشتمل ہو۔


Volume Password

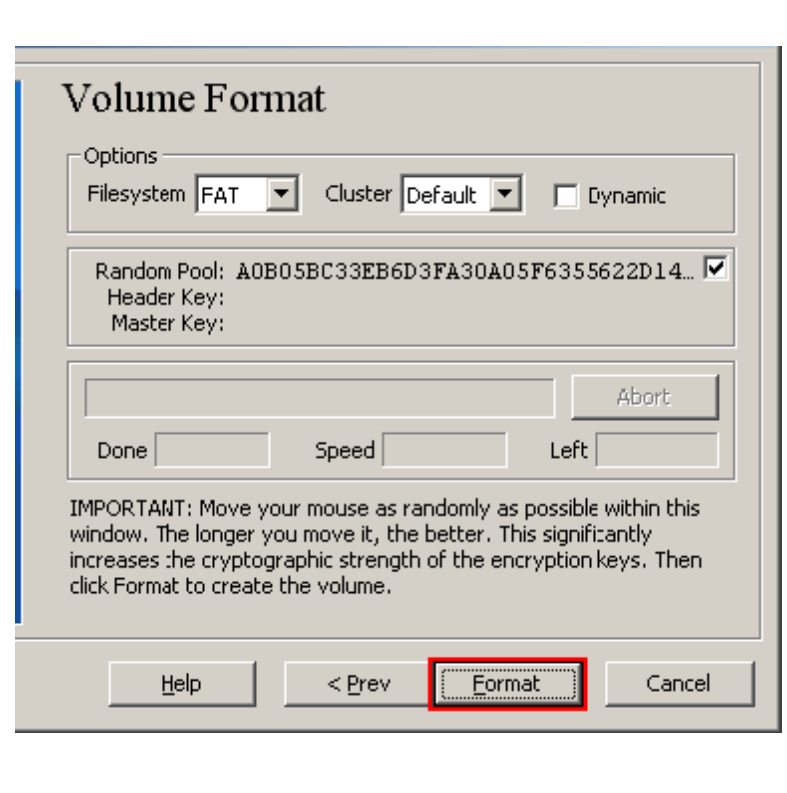
Password:

Confirm:

☐ Display password
☐ Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.

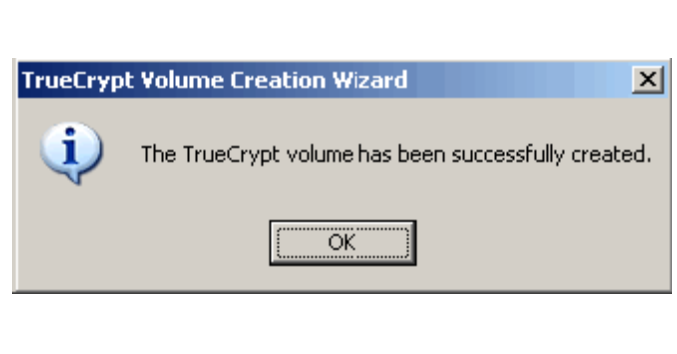
ماؤس کو نیچے دکھائی گئی ونڈو پر تیزی سے کافی دیر تک حرکت دیں تاکہ مضبوط key تیار ہو سکے


Volume Format

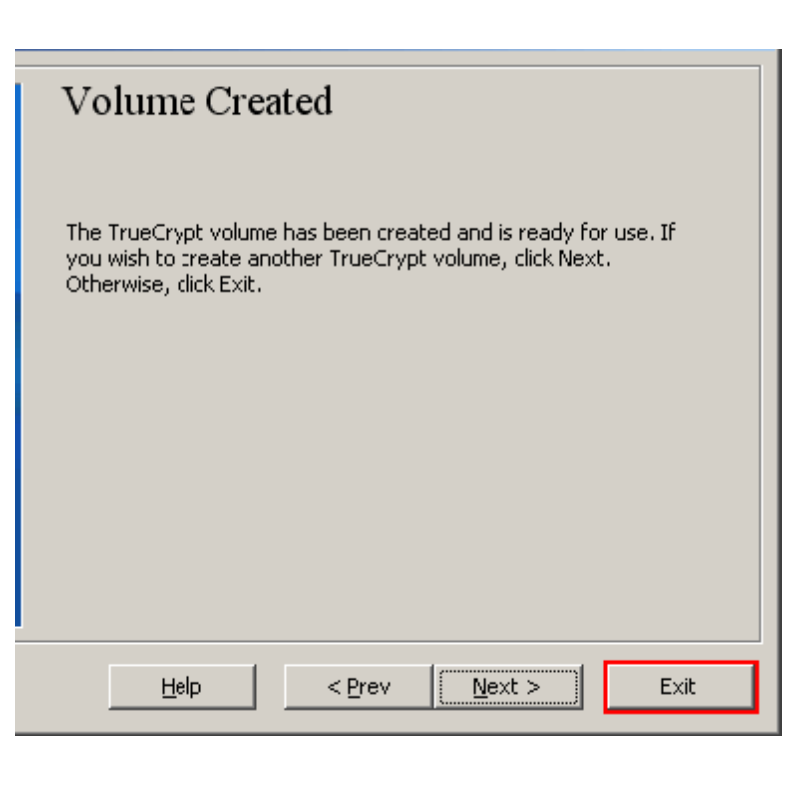
Options: Filesystem FAT, Cluster Default, ☐ Dynamic

Random Pool: A0B05BC33EB6D3FA30A05F6355622D14... ☑
Header Key:
Master Key:

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.


TrueCrypt Volume Creation Wizard

The TrueCrypt volume has been successfully created.

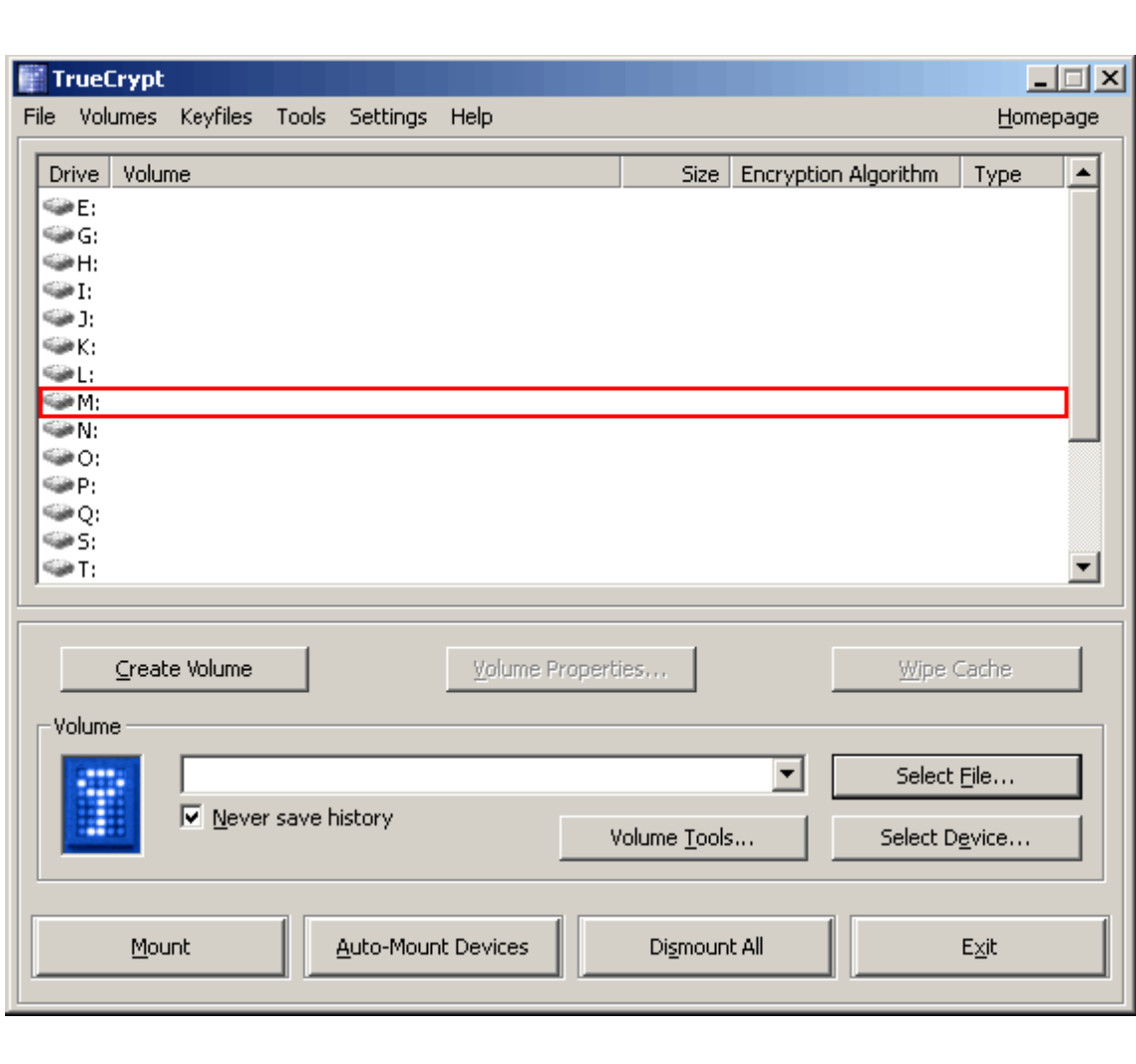

Volume Created

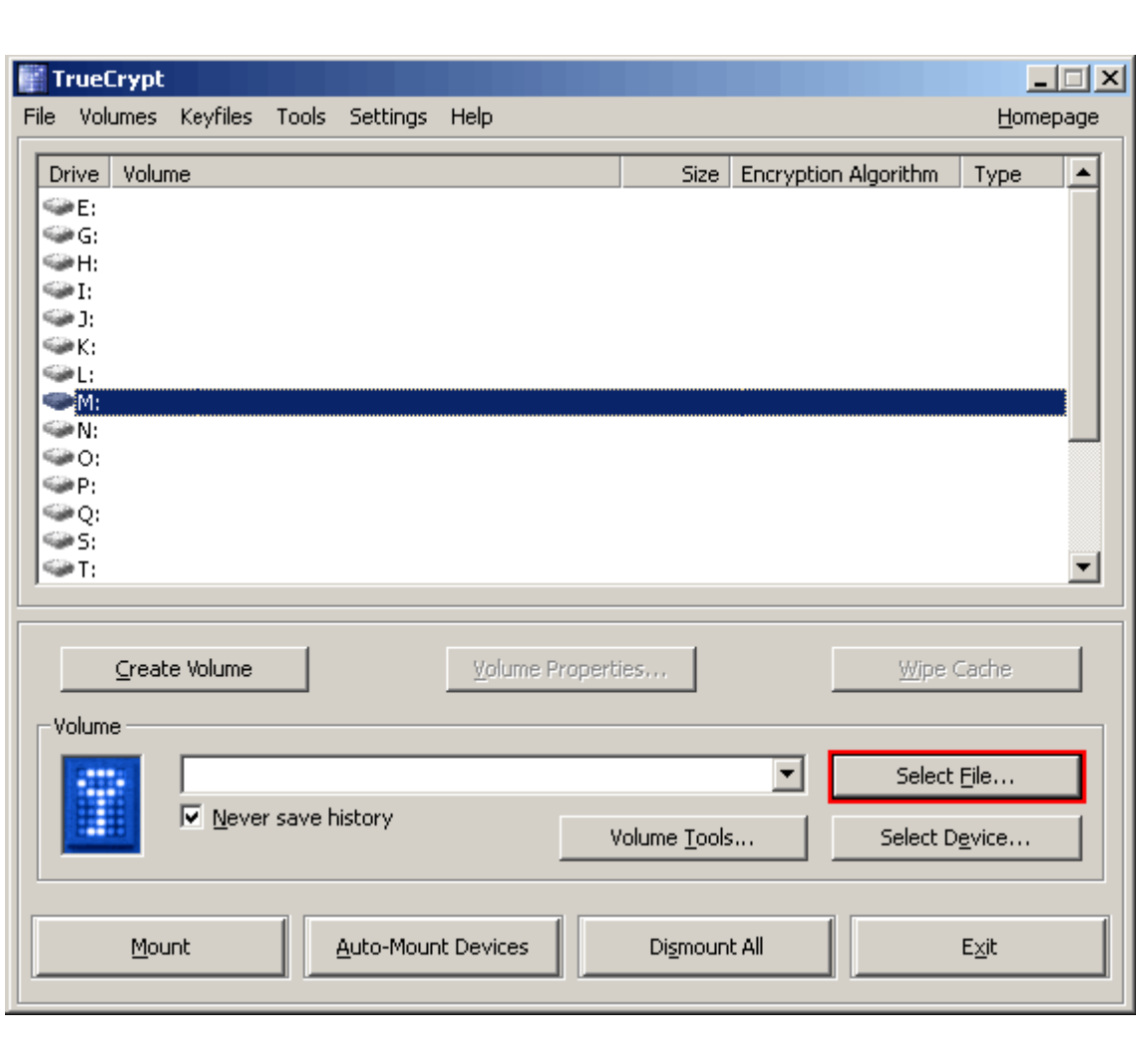
The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.

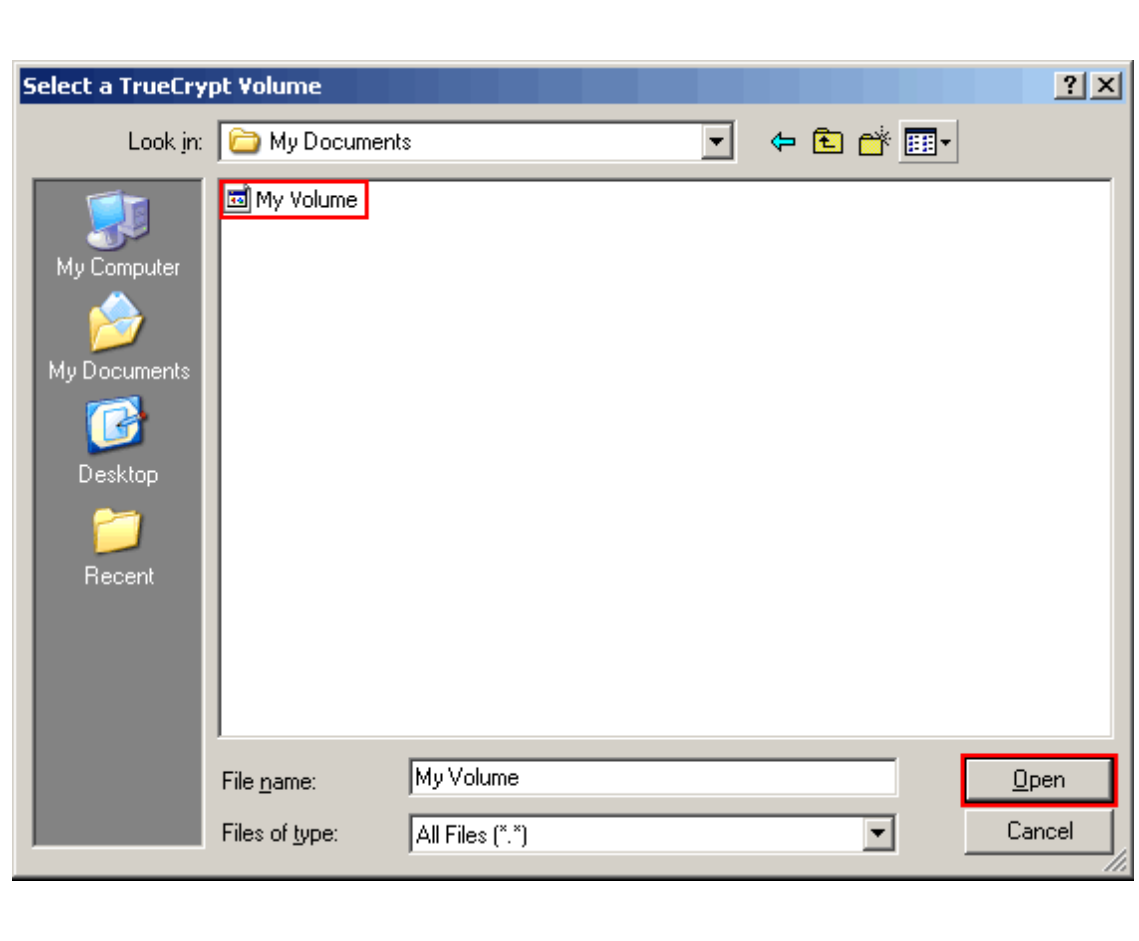
کنٹینر آپ کی بتائی ہوئی جگہ پر بن چکا ہے۔ کنٹینر اسی سائز کا بنا ہے جتنا کہا تھا اگرچہ یہ ابھی اندر سے بالکل خالی ہے۔ اور یہ اندازہ لگانا ناممکن ہے کہ فی الوقت کنٹینر میں کتنا ڈیٹا موجود ہے۔

My Volume
File
15,360 KB

کنٹینر کھولنے (یعنی mount کرنے) کا طریقہ


TrueCrypt


TrueCrypt

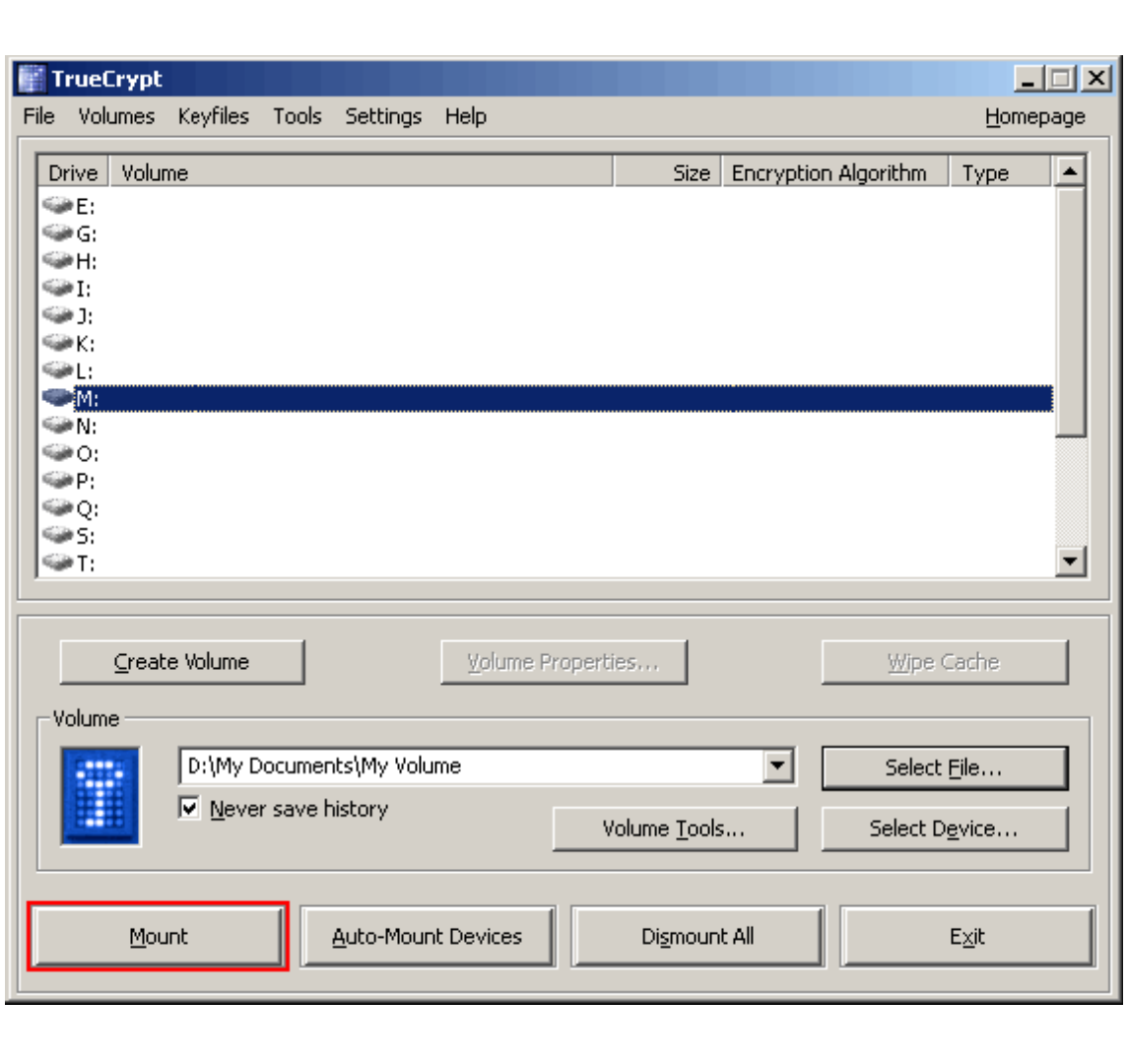

Select a TrueCrypt Volume

Look in: My Documents

My Volume

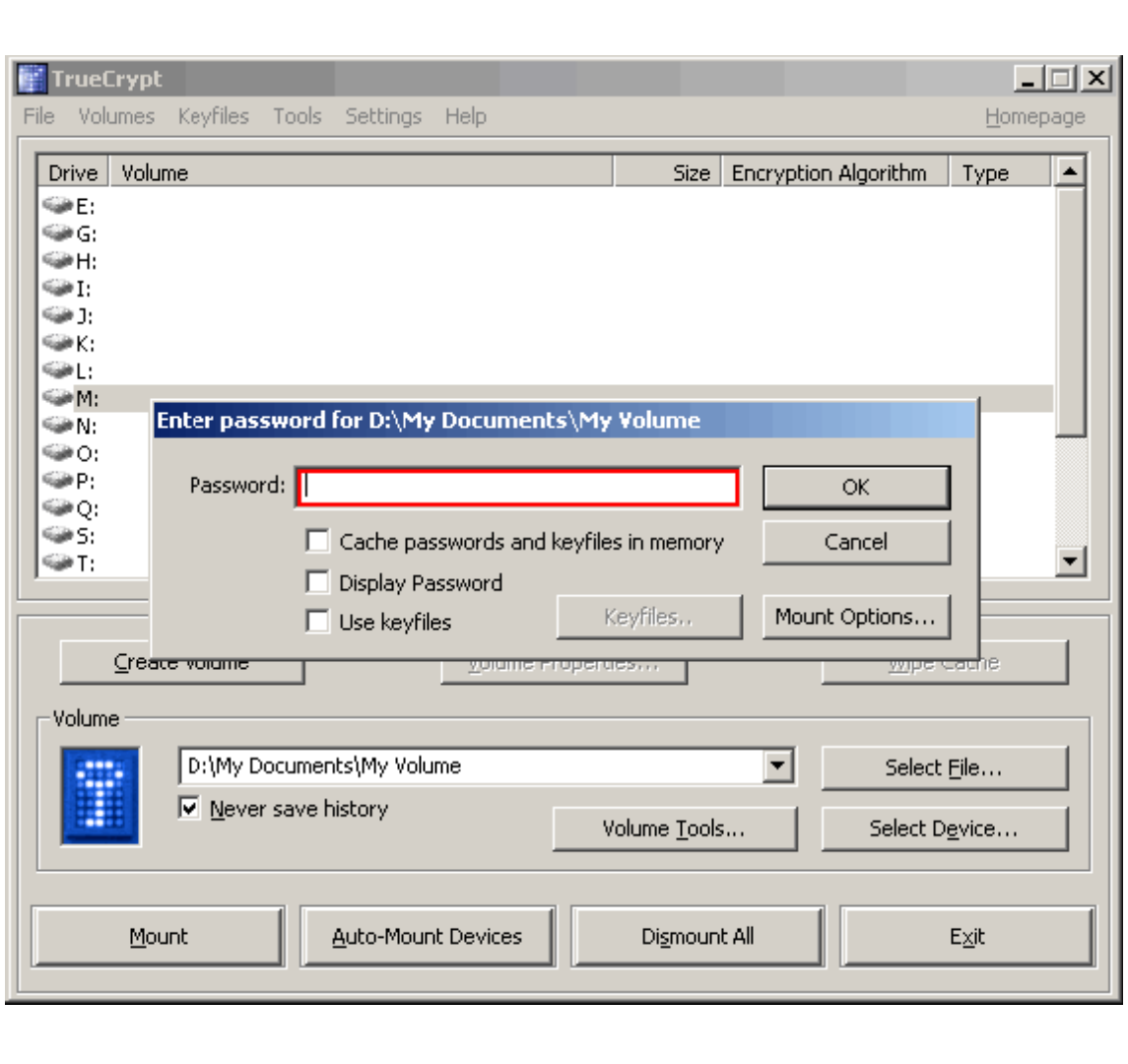
File name: My Volume

Files of type: All Files (*.*)


TrueCrypt

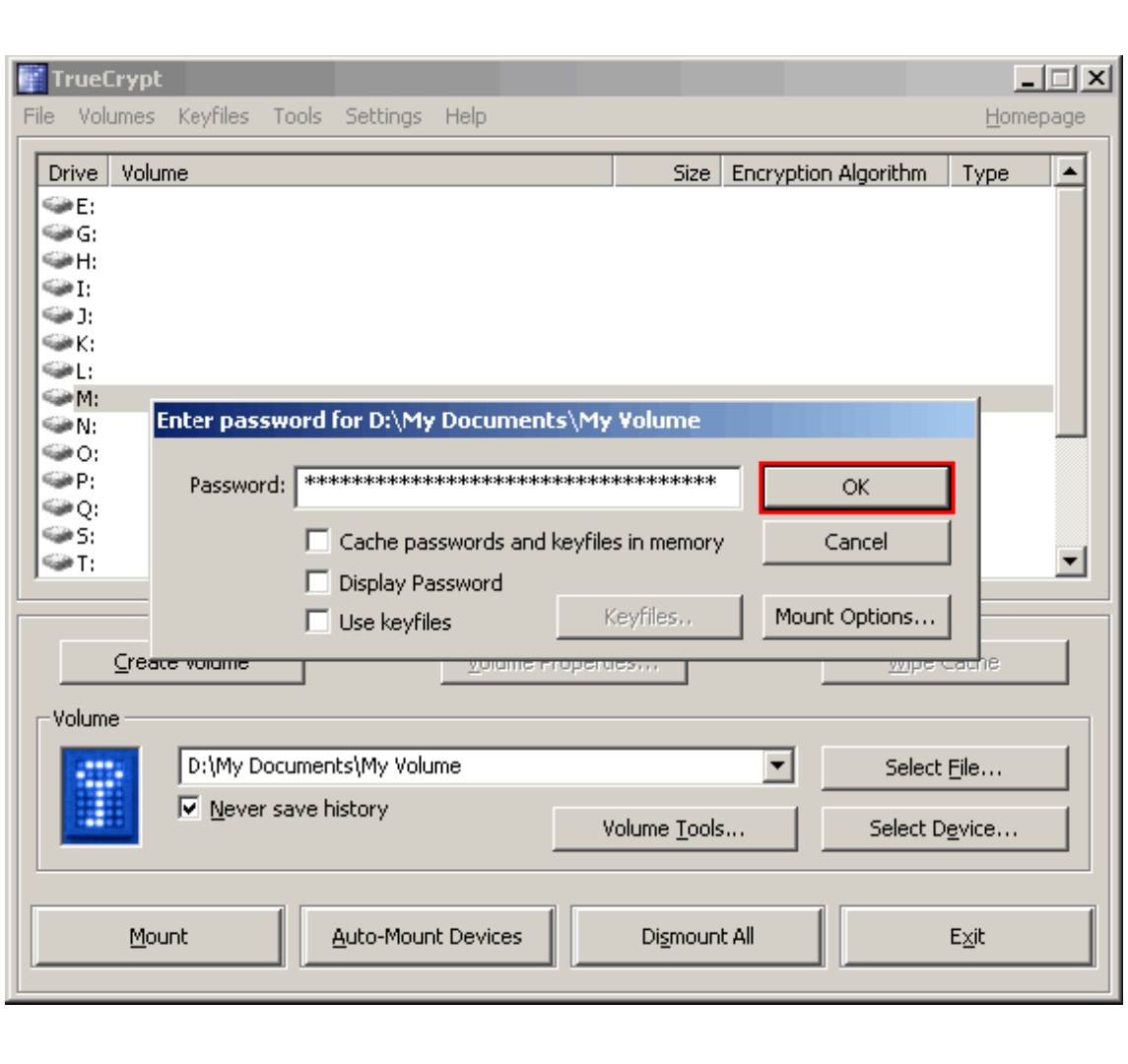
D:\My Documents\My Volume

☑ Never save history


Enter password for D:\My Documents\My Volume

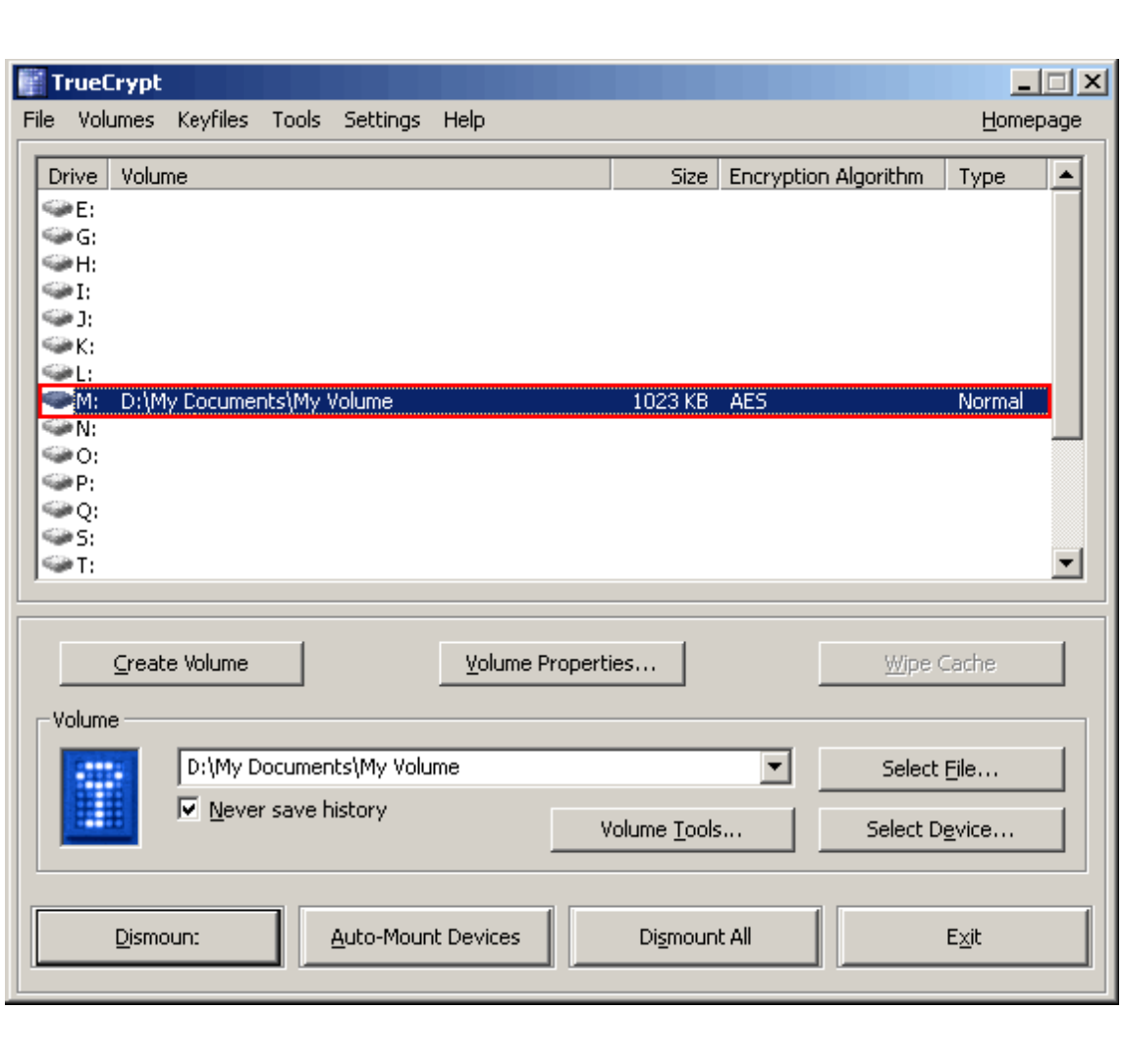
Password:

☐ Cache passwords and keyfiles in memory
☐ Display Password
☐ Use keyfiles


Enter password for D:\My Documents\My Volume

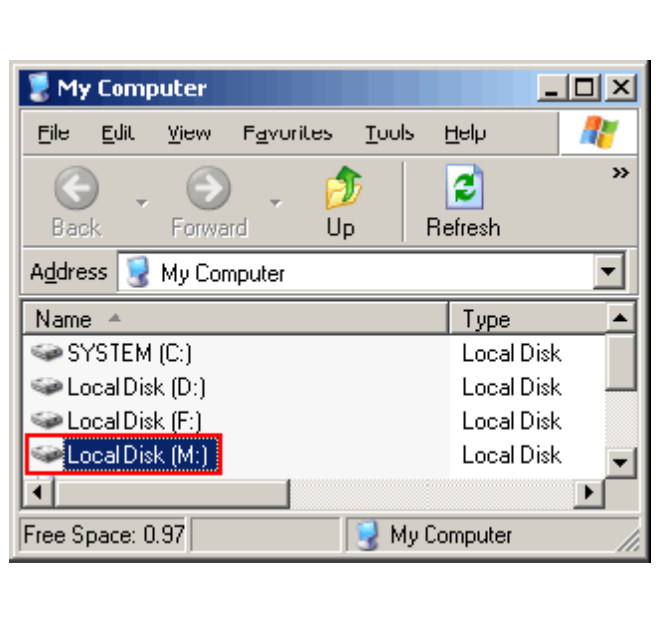
Password: ************************************

☐ Cache passwords and keyfiles in memory
☐ Display Password
☐ Use keyfiles


TrueCrypt

M: D:\My Documents\My Volume 1023 KB AES Normal

کنٹینر ماؤنٹ (mount) ہو چکا ہے۔ جیسے کمپیوٹر میں دیگر ڈرائیوز ہیں ویسے ہی ایک ڈرائیو آپ کے کنٹینر کی بن گئی ہے۔ اب جو ڈیٹا بھی اس میں کاپی کیا جائے گا وہ اینکرپٹ ہو کر اس میں چلا جائے گا۔

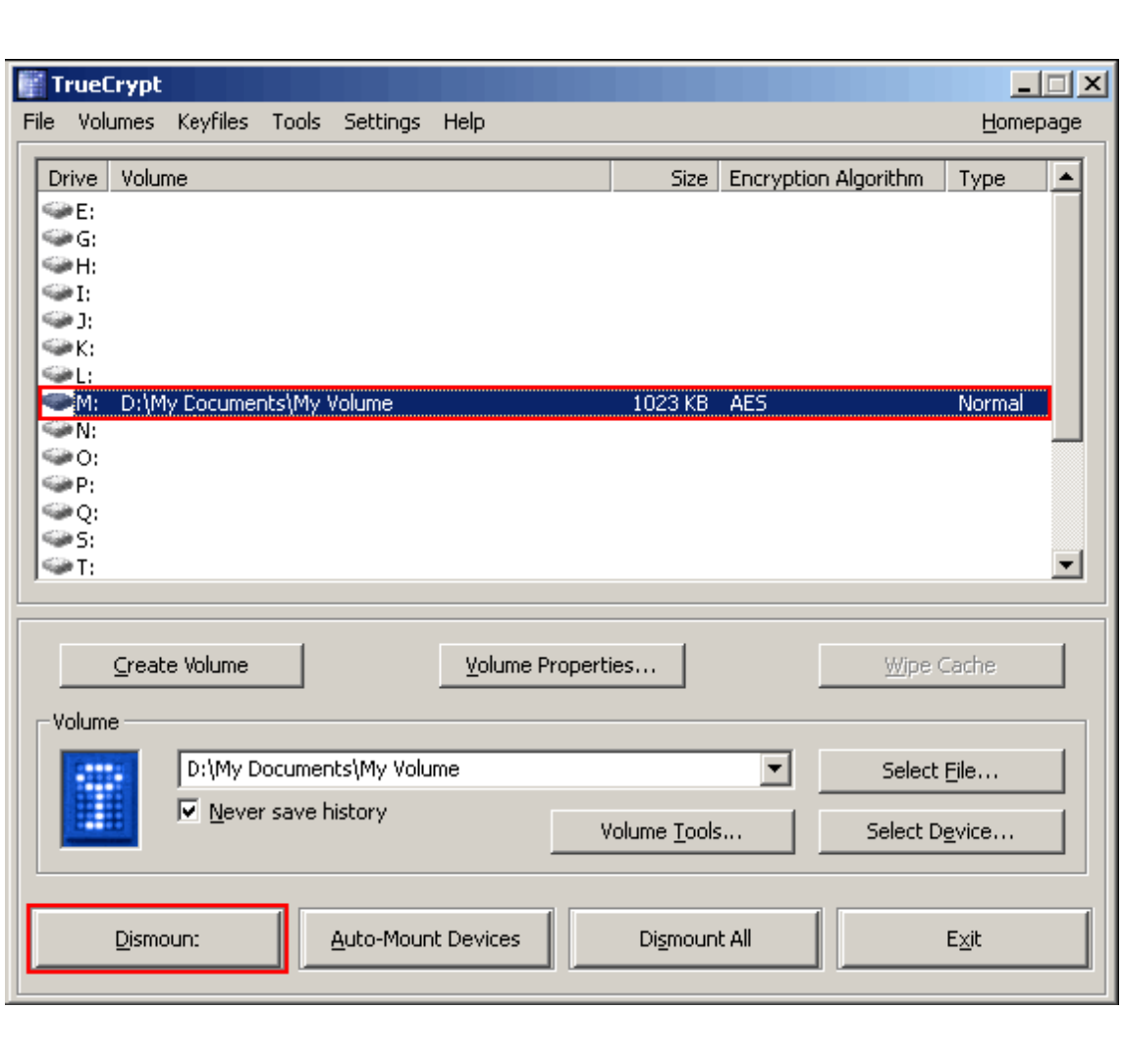

My Computer

Name	Type
SYSTEM (C:)	Local Disk
Local Disk (D:)	Local Disk
Local Disk (F:)	Local Disk
Local Disk (M:)	Local Disk

Free Space: 0.97

یاد رہے اگرچہ کنٹینر ماؤنٹ ہو چکا ہے اور اس میں پڑا ڈیٹا عام انداز میں دیکھا جا سکتا ہے مگر اس وقت وہ سارا ڈیٹا / فائیلیں جو کنٹینر کے اندر موجود ہیں وہ اینکرپٹڈ حالت میں ہی ہیں۔

کنٹینر بند (یعنی dismount کرنے) کا طریقہ


TrueCrypt

M: D:\My Documents\My Volume 1023 KB AES Normal

D:\My Documents\My Volume

TrueCrypt میں چھپا ہوا کنٹینر (یعنی Hidden کنٹینر) بنانے کا طریقہ

TrueCrypt میں چھپا ہوا کنٹیز (یعنی Hidden کنٹیز) بنانے کا طریقہ

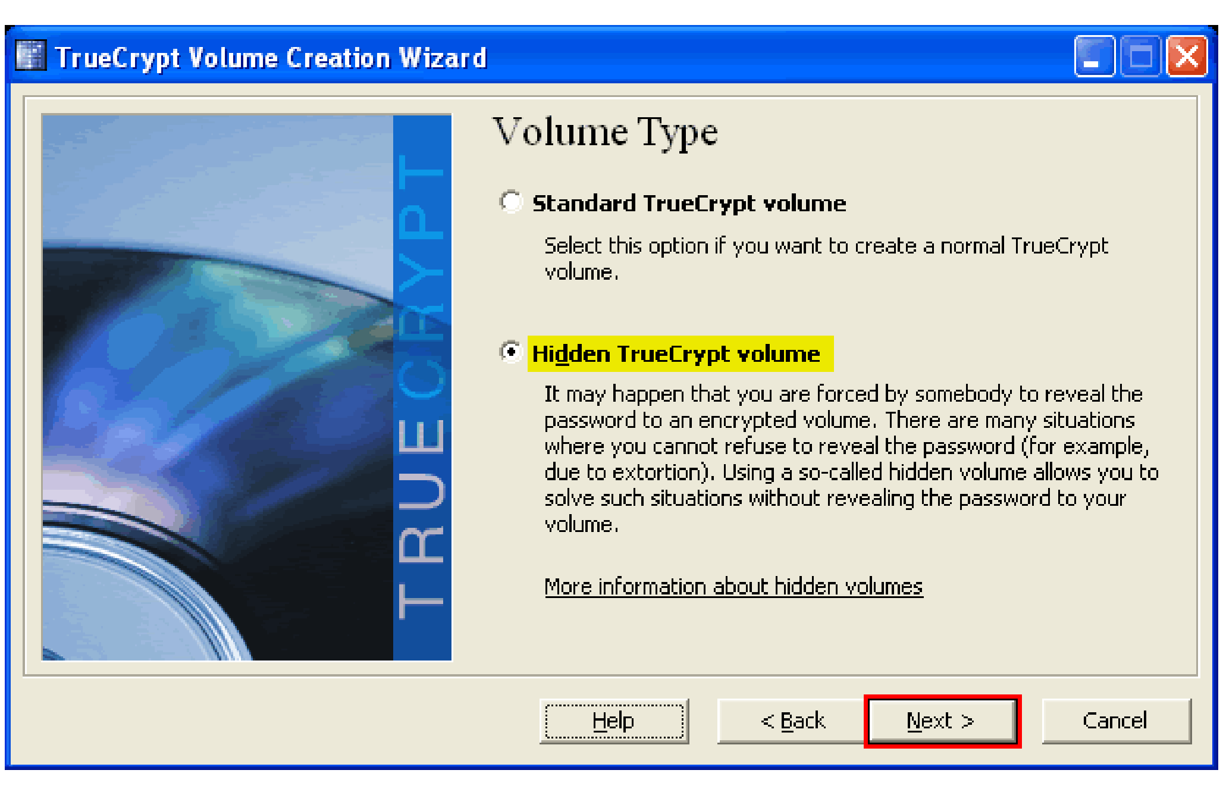
جہاں TrueCrypt کے ذریعے ہم اپنے ڈیٹا کو انکرپٹڈ حالت میں محفوظ رکھ سکتے ہیں، وہیں کبھی ایسی صورت حال بھی پیدا ہو سکتی ہے کہ کسی سے اس کا پاسورڈ زبردستی اگلوایا جائے۔ اور اُس کے پاس پاسورڈ عیاں کرنے کے علاوہ اور کوئی چارہ نہ ہو۔ ایسی صورتحال کیلئے TrueCrypt کے کنٹیز میں ایک Hidden کنٹیز بنا لینا بہت فائدہ مند ثابت ہو سکتا ہے۔

Hidden کنٹیز، عام کنٹیز کے اندر ہی ایک کنٹیز ہوتا ہے، اور یہ بات کسی صورت ثابت نہیں کی جا سکتی کہ اس کنٹیز کے اندر کوئی Hidden کنٹیز بھی موجود ہے۔ اس طرح ہم حساس ڈیٹا کو Hidden کنٹیز میں رکھ کر ایسی صورتحال کا مقابلہ کر سکتے ہیں۔

Hidden کنٹیز اور باہر کے کنٹیز (یعنی عام کنٹیز) میں استعمال کا صرف اتنا فرق ہے کہ اگر آپ عام کنٹیز (یعنی بیرونی یا Outer کنٹیز) کا پاسورڈ ڈالیں گے تو Outer کنٹیز ماؤنٹ ہو جائے گا اور اگر Hidden کنٹیز کا پاسورڈ ڈالیں گے تو Hidden کنٹیز ماؤنٹ ہو جائے گا۔

Hidden کنٹیز کیسے بنایا جائے ؟

کنٹیز بناتے وقت TrueCrypt ہمیں یہ آپشن دیتا ہے کہ ہم هیڈن کنٹیز بنا سکیں:


TrueCrypt Volume Creation Wizard

Volume Type

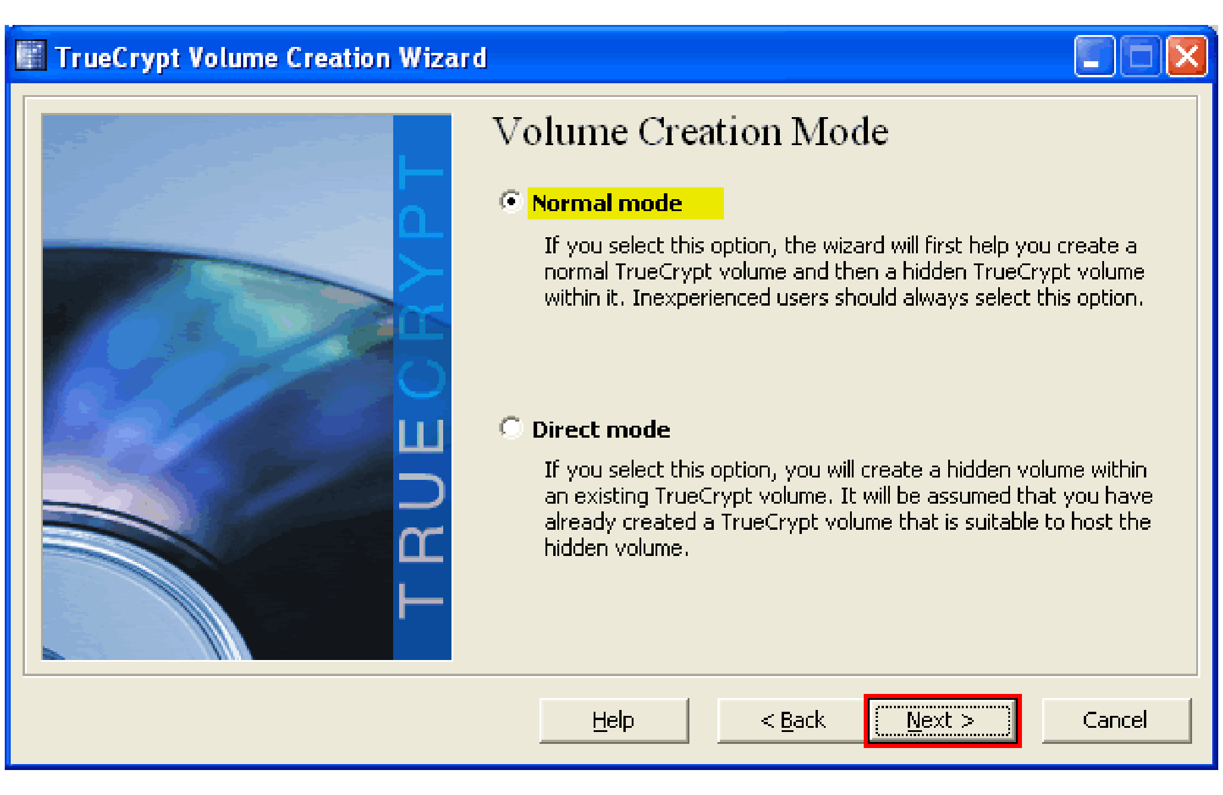
○ Standard TrueCrypt volume

Select this option if you want to create a normal TrueCrypt volume.

● Hidden TrueCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes


TrueCrypt Volume Creation Wizard

Volume Creation Mode

● Normal mode

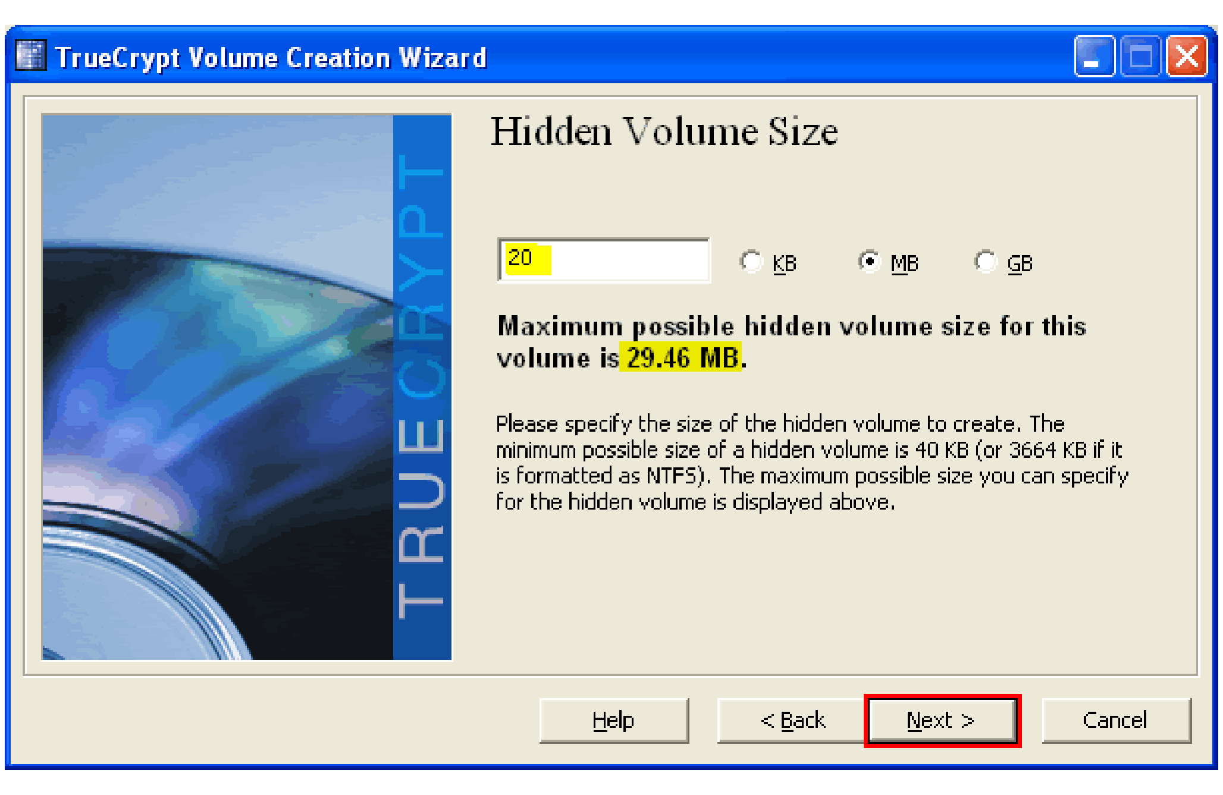
If you select this option, the wizard will first help you create a normal TrueCrypt volume and then a hidden TrueCrypt volume within it. Inexperienced users should always select this option.

○ Direct mode

If you select this option, you will create a hidden volume within an existing TrueCrypt volume. It will be assumed that you have already created a TrueCrypt volume that is suitable to host the hidden volume.

اس کے بعد کا مرحلہ ویسا ہی ہے جیسے عام کنٹیز کا ہے، اس طریقے میں پہلے عام کنٹیز بنے گا پھر هیڈن کنٹیز۔ دونوں کیلئے علیحدہ بار پاسورڈ مانگے جائیں گے۔ (TrueCrypt یہ آپشن بھی دیتا ہے کہ آپ پہلے سے بنے کنٹیز میں هیڈن کنٹیز بنا سکیں۔)

هیڈن کنٹیز کا سائز زیادہ سے زیادہ اتنا ہی ہو سکتا ہے جتنا کہ Outer کنٹیز کا، کیونکہ اس نے Outer کنٹیز کے اندر بننا ہے۔


TrueCrypt Volume Creation Wizard

Hidden Volume Size

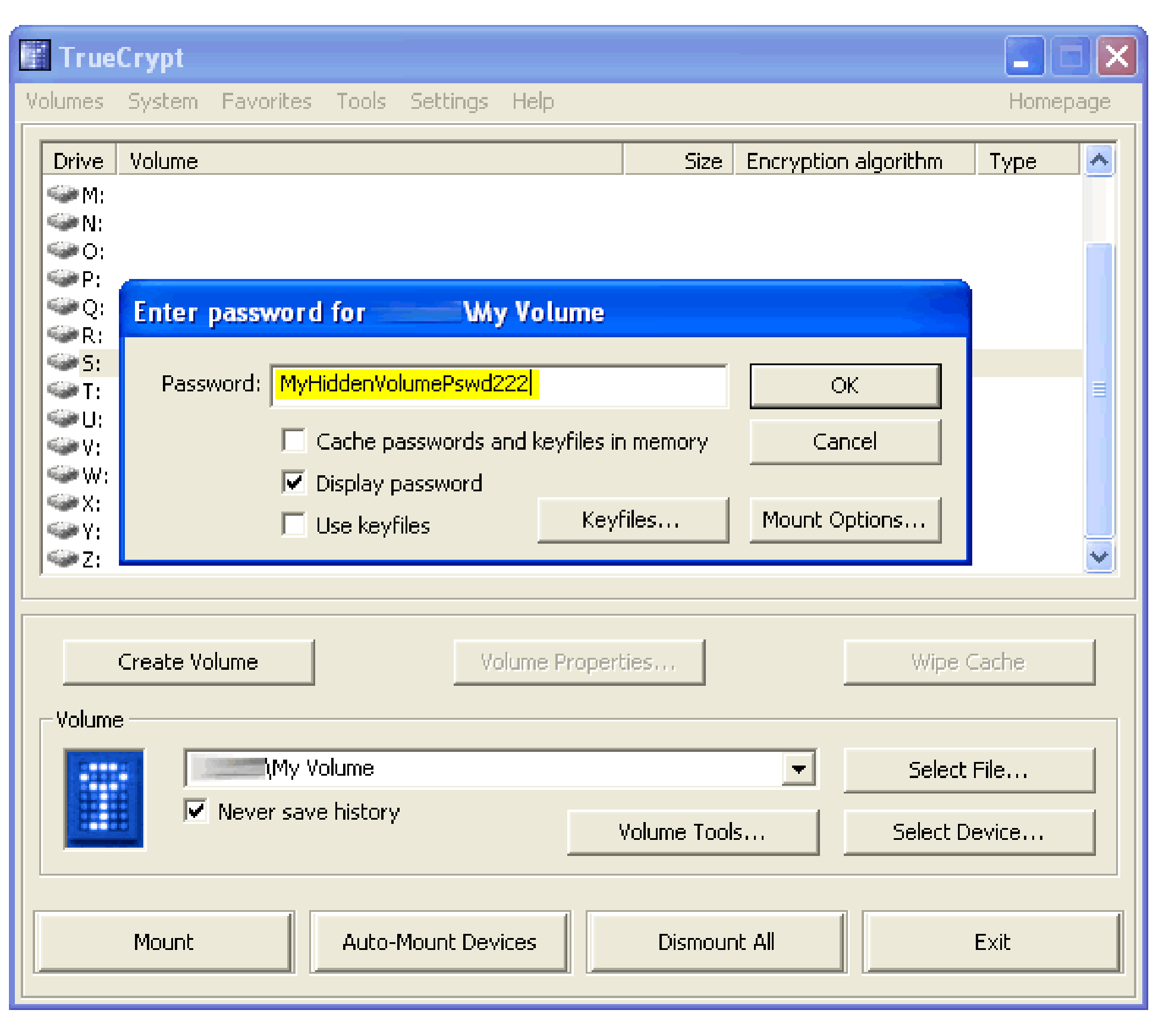
20 ○ KB ● MB ○ GB

Maximum possible hidden volume size for this volume is 29.46 MB.

Please specify the size of the hidden volume to create. The minimum possible size of a hidden volume is 40 KB (or 3664 KB if it is formatted as NTFS). The maximum possible size you can specify for the hidden volume is displayed above.

کنٹیز کھولنے (یعنی ماؤنٹ کرنے) کا طریقہ:

جب آپ هیڈن کنٹیز کھولنا چاہتے ہیں تو هیڈن کنٹیز کا پاسورڈ درج کریں گے، هیڈن کنٹیز ماؤنٹ ہو جائے گا۔

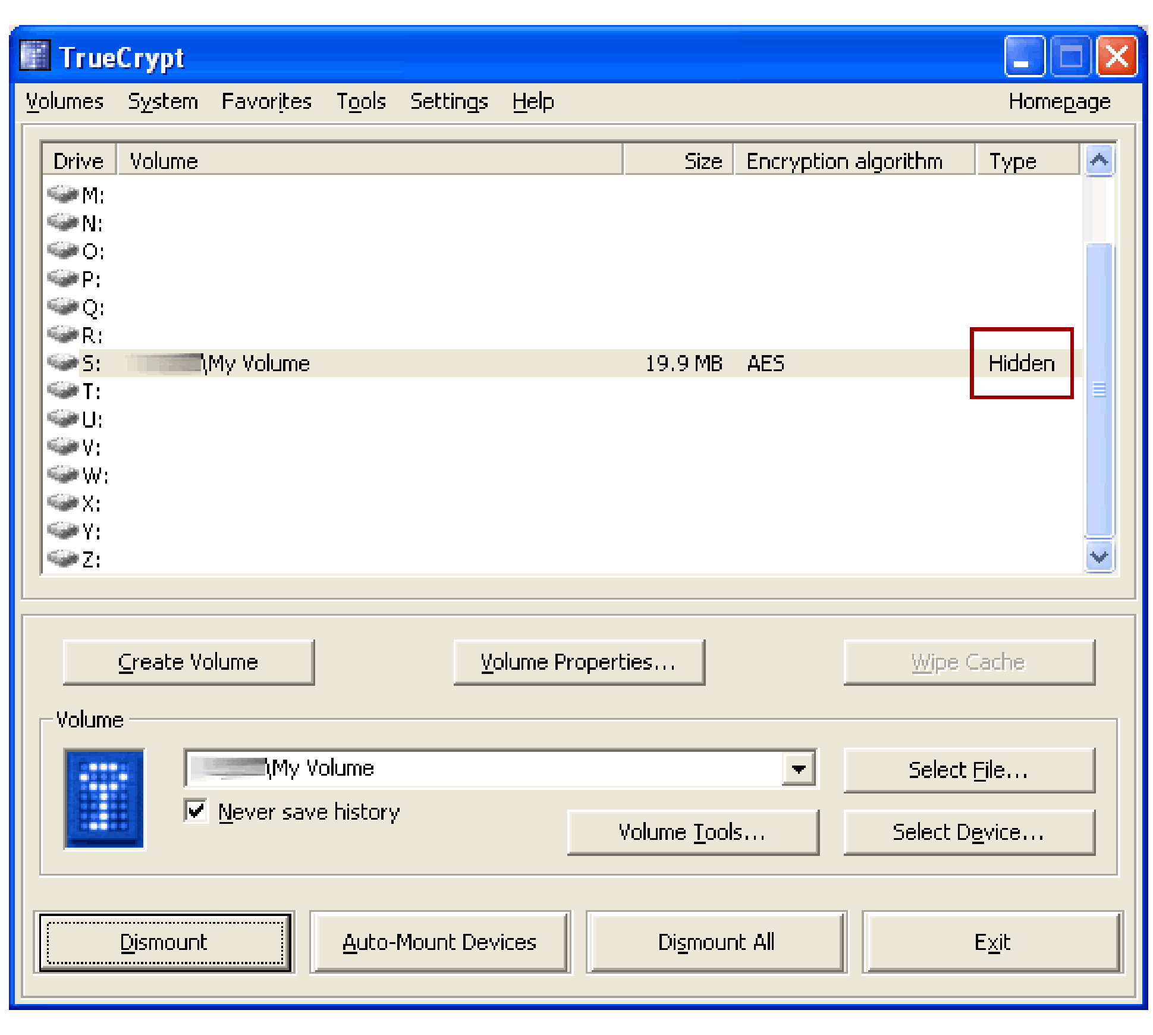

Enter password for \My Volume

Password: MyHiddenVolumePswd222

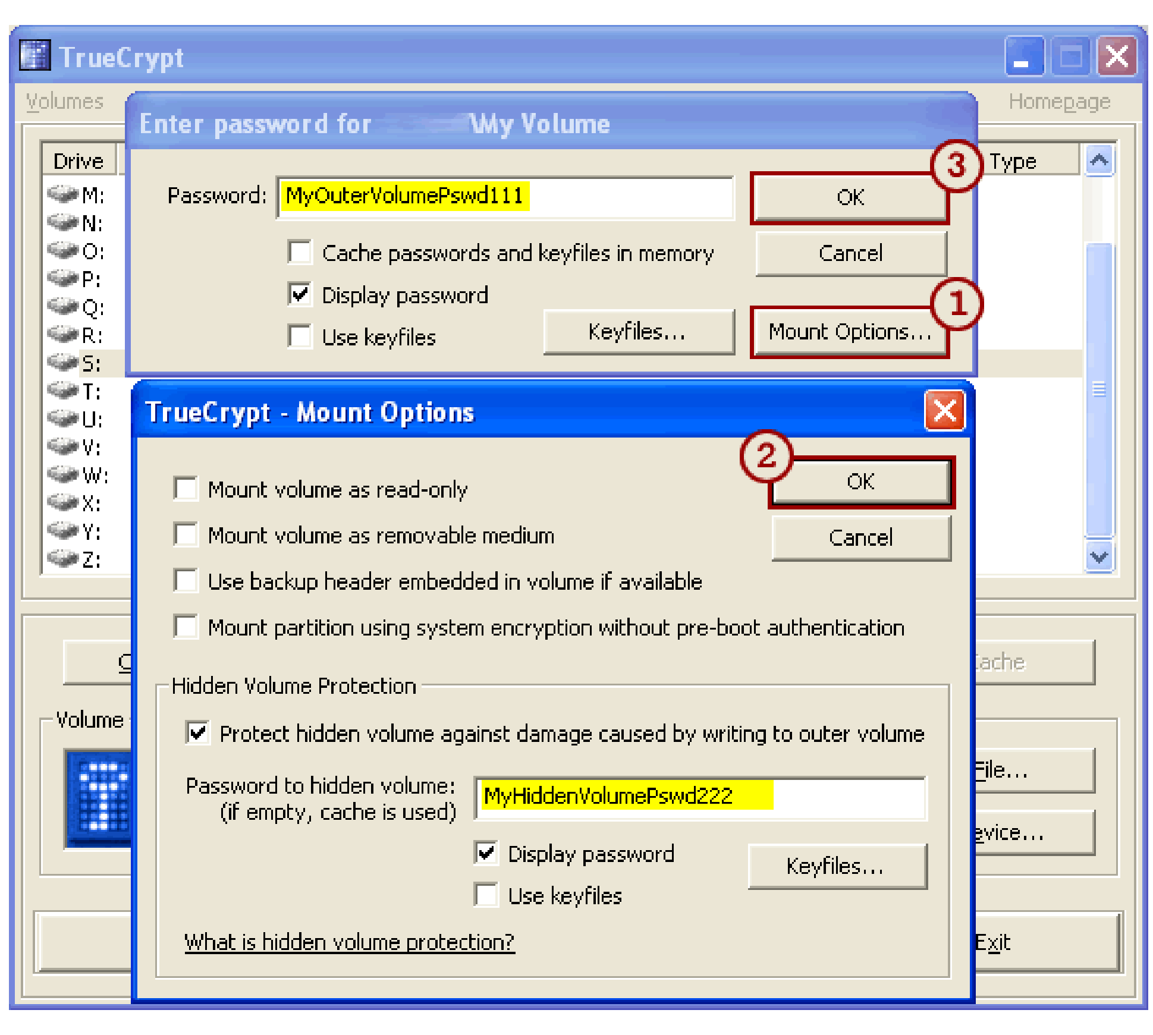
☐ Cache passwords and keyfiles in memory

☑ Display password

☐ Use keyfiles


Drive	Volume	Size	Encryption algorithm	Type
S:	\My Volume	19.9 MB	AES	Hidden

لیکن جب آپ Outer کنٹیز کھولنا چاہیں گے تو ساتھ هیڈن کنٹیز کا پاسورڈ ڈال کر TrueCrypt کو یہ بتائیں گے کہ اس میں ایک هیڈن کنٹیز بھی ہے، اور کہیں ایسا نہ ہو کہ میں Outer کنٹیز میں ڈیٹا ڈالتا رہوں اور TrueCrypt کو پتہ ہی نہ چلے کہ اس میں کوئی هیڈن بھی ہے اور وہ بے خبری میں میرے هیڈن کنٹیز کی جگہ پر بھی ڈیٹا رائٹ کر دے، اور یوں میرا هیڈن کنٹیز کا ڈیٹا ضائع (corrupt) ہو جائے۔


Enter password for \My Volume

Password: MyOuterVolumePswd111

☐ Cache passwords and keyfiles in memory

☑ Display password

☐ Use keyfiles

TrueCrypt - Mount Options

☐ Mount volume as read-only

☐ Mount volume as removable medium

☐ Use backup header embedded in volume if available

☐ Mount partition using system encryption without pre-boot authentication

Hidden Volume Protection

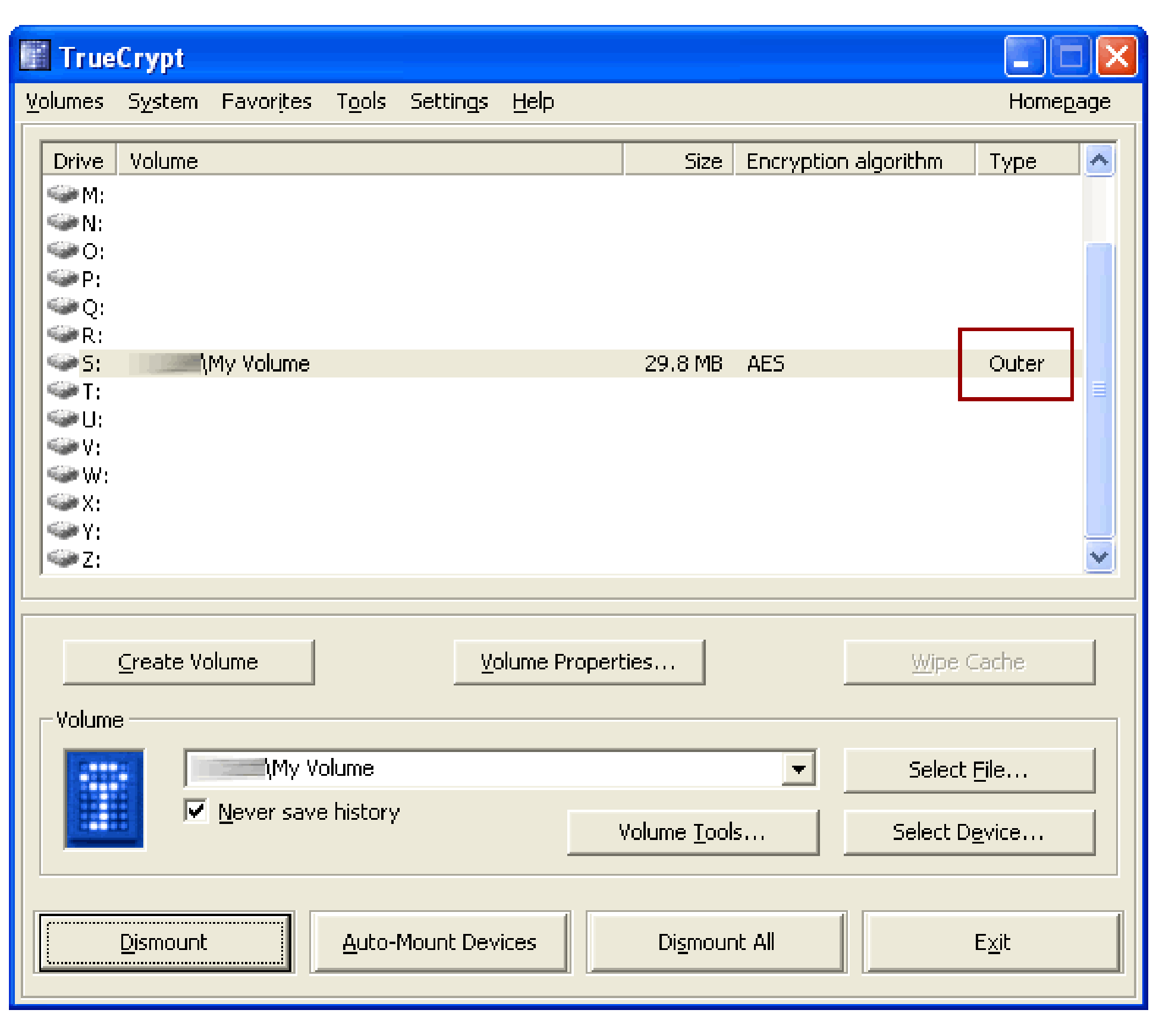
☑ Protect hidden volume against damage caused by writing to outer volume

Password to hidden volume: (if empty, cache is used) MyHiddenVolumePswd222

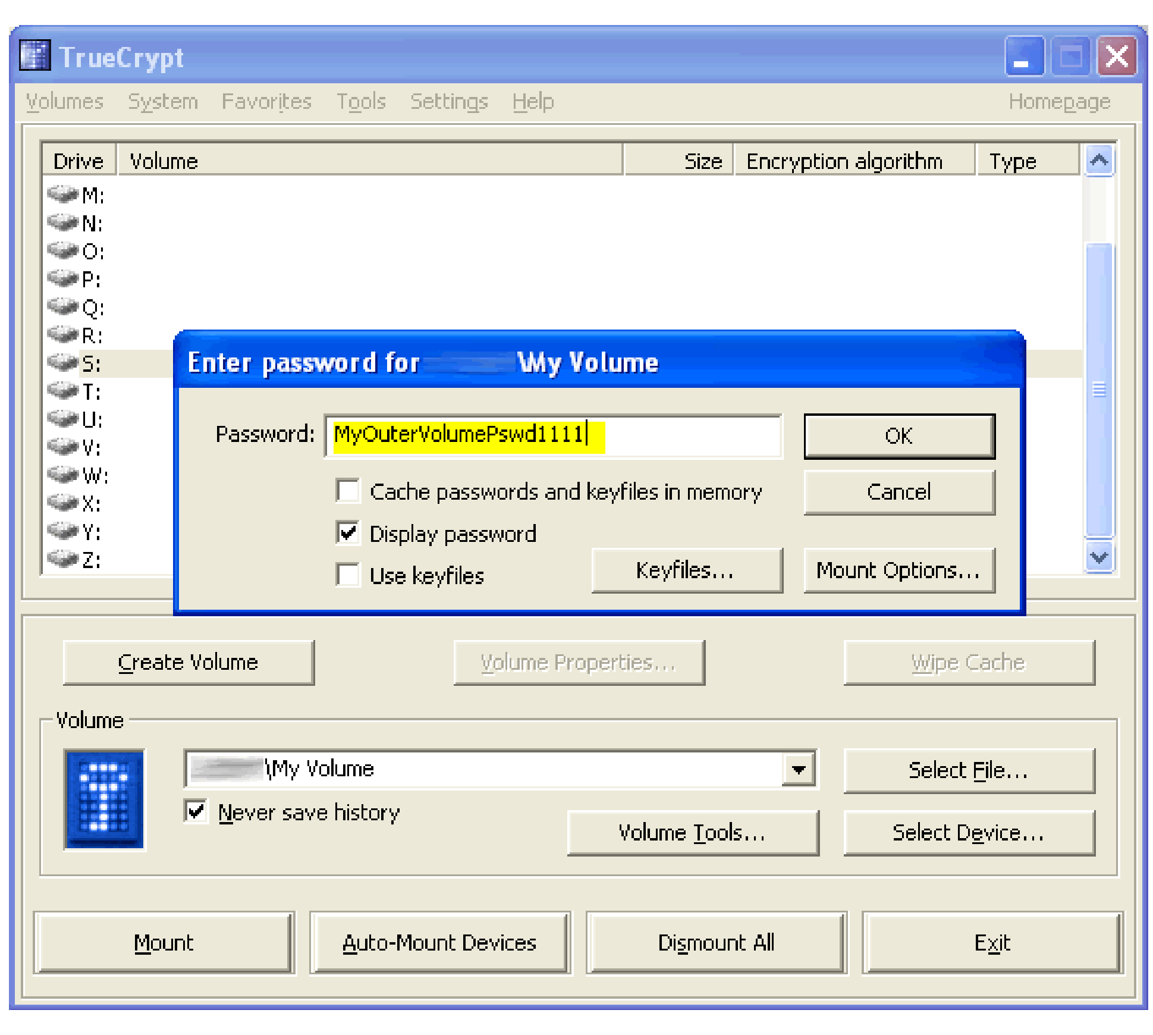
☑ Display password

☐ Use keyfiles

What is hidden volume protection?


Drive	Volume	Size	Encryption algorithm	Type
S:	\My Volume	29.8 MB	AES	Outer

لیکن ایسا تب نہیں کیا جائے گا جب کسی سے پاسورڈ زبردستی ڈالنے کو کہا جائے۔ تب کنٹیز کو ایسے ہی Outer کنٹیز کا پاسورڈ ڈال کر کھولا جائے گا جیسے عام کنٹیز کھولے جاتے ہیں۔ اور TrueCrypt میں ڈرائیو کے سامنے ویسے ہی Normal لکھا آئے گا جیسے یہ عام طریقے میں لکھا آتا ہے۔اس طریقے سے کنٹیز بھی کھل جائے گا (جو کہ آؤٹر کنٹیز ہو گا) اور حساس ڈیٹا بھی نظروں کے سامنے نہیں آئے گا (کیونکہ هیڈن کنٹیز ابھی بھی چھپا ہوا ہے)۔

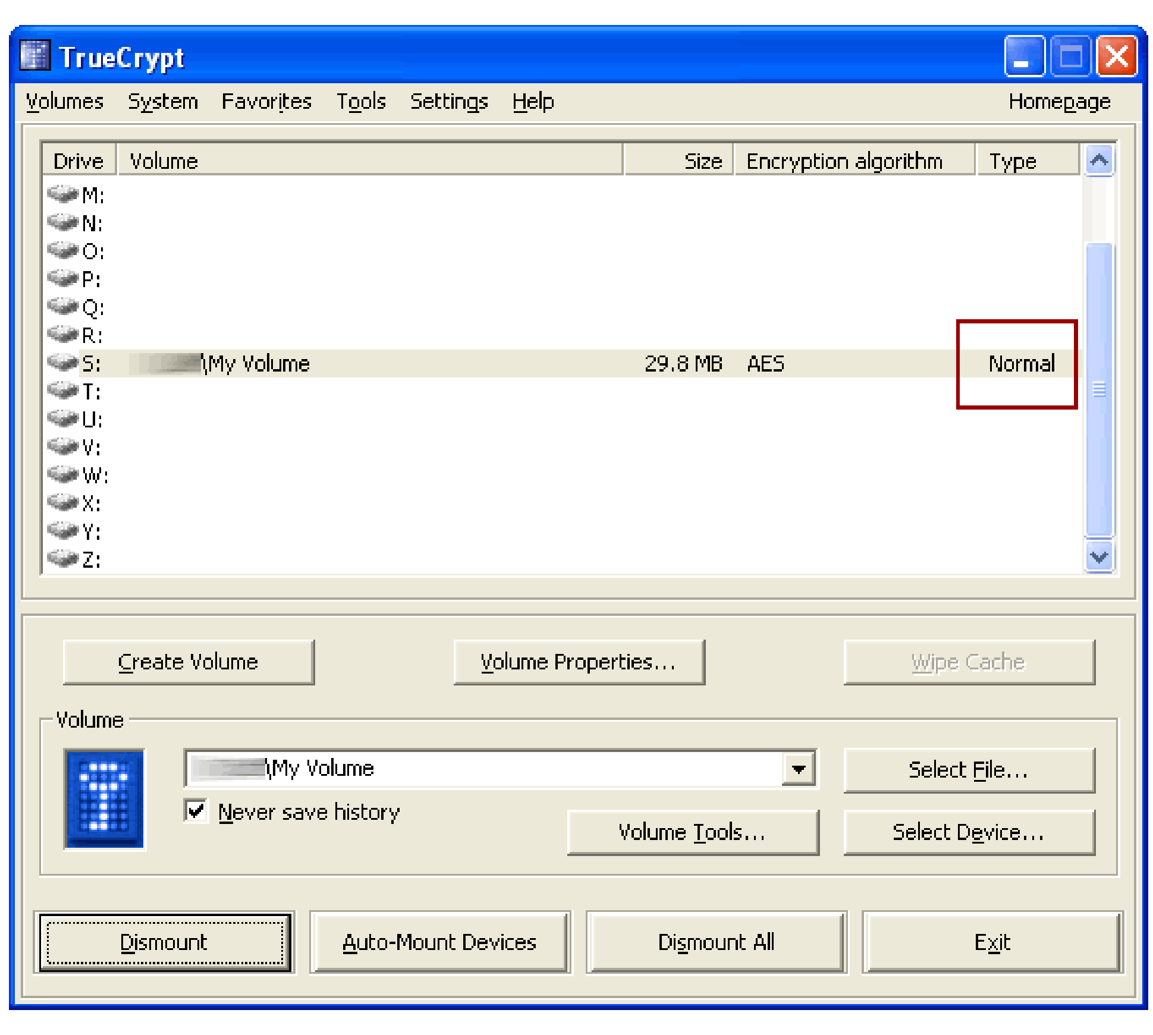

Enter password for \My Volume

Password: MyOuterVolumePswd1111

☐ Cache passwords and keyfiles in memory

☑ Display password

☐ Use keyfiles


Drive	Volume	Size	Encryption algorithm	Type
S:	\My Volume	29.8 MB	AES	Normal
